

(19) 世界知的所有権機関  
国際事務局(43) 国際公開日  
2006年4月20日 (20.04.2006)

PCT

(10) 国際公開番号  
WO 2006/040798 A1

- (51) 国際特許分類<sup>7</sup>: G06F 12/14
- (21) 国際出願番号: PCT/JP2004/014939
- (22) 国際出願日: 2004年10月8日 (08.10.2004)
- (25) 国際出願の言語: 日本語
- (26) 国際公開の言語: 日本語
- (71) 出願人 (米国を除く全ての指定国について): 株式会社ルネサステクノロジ (RENESAS TECHNOLOGY CORP.) [JP/JP]; 〒1006334 東京都千代田区丸の内二丁目4番1号 Tokyo (JP).
- (72) 発明者; および
- (75) 発明者/出願人 (米国についてのみ): 大柴 雅史 (OSHIBA, Masashi) [JP/JP]; 〒1006334 東京都千代田区丸の内二丁目4番1号株式会社ルネサステクノロジ内 Tokyo (JP). 岸 洋司 (KISHI, Hiroshi) [JP/JP]; 〒1006334

東京都千代田区丸の内二丁目4番1号株式会社ルネサステクノロジ内 Tokyo (JP). 佐藤 芳彰 (SATO, Yoshiaki) [JP/JP]; 〒0668511 北海道千歳市泉沢1007番地39株式会社ルネサス北日本セミコンダクタ内 Hokkaido (JP). 山本 陽子 (YAMAKI, Yoko) [JP/JP]; 〒0668511 北海道千歳市泉沢1007番地39株式会社ルネサス北日本セミコンダクタ内 Hokkaido (JP). 山川 健太郎 (YAMAKAWA, Kentaro) [JP/JP]; 〒0668511 北海道千歳市泉沢1007番地39株式会社ルネサス北日本セミコンダクタ内 Hokkaido (JP).

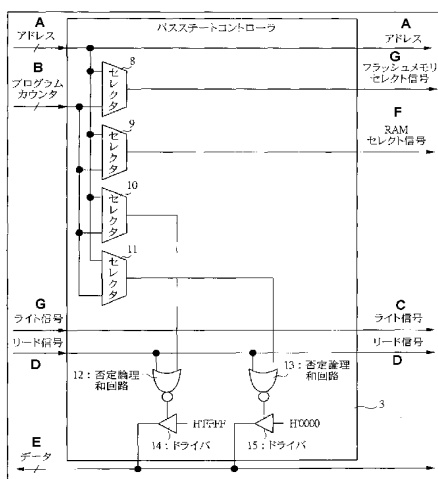
(74) 代理人: 筒井 大和 (TSUTSUI, Yamato); 〒1600023 東京都新宿区西新宿8丁目1番1号アゼリアビル3階 筒井国際特許事務所 Tokyo (JP).

(81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR,

[続葉有]

(54) Title: SEMICONDUCTOR INTEGRATED CIRCUIT DEVICE AND ELECTRONIC SYSTEM

(54) 発明の名称: 半導体集積回路装置および電子システム



A.. ADDRESS  
B.. PROGRAM COUNTER  
C.. WRITE SIGNAL  
D.. READ SIGNAL  
E.. DATA  
3.. BUS STATE CONTROLLER  
8.. SELECTOR  
9.. SELECTOR  
10.. SELECTOR  
11.. SELECTOR  
12.. NEGATIVE OR CIRCUIT  
13.. NEGATIVE OR CIRCUIT  
14.. DRIVER  
15.. DRIVER  
F.. RAM SELECT SIGNAL  
G.. FLASH MEMORY SELECT SIGNAL

(57) Abstract: A flash memory includes a protect area (PA) where reading of specified blocks is inhibited, while a RAM, which is used as a work area of a program, also includes a protect area (PA1) where reading of specified blocks is inhibited. A bus state controller (3) compares the value of a program counter with the value of an address signal to inhibit reading from the areas other than the protect area (PA) for the flash memory and to control the data of the protect area (PA1) for the RAM such that reading from the protect area (PA) in the flash memory is inhibited. For example, if a user is to read the data of the protect area (PA) from an accessible user access area, meaningless data, such as H'FFFF or the like, is outputted from the bus state controller (3) via a data bus.

(57) 要約: フラッシュメモリには、特定のブロックの読み出しが禁止されるプロテクトエリアPAが設けられ、プログラムのワークエリアとして用いられるRAMには、同じく特定のブロックの読み出しが禁止されるプロテクトエリアPA1が設けられている。バスステートコントローラ3は、プログラムカウンタの値とアドレス信号の値とを比較して、フラッシュメモリではプロテクトエリアPA以外の読み出しを禁止し、RAMではプロテクトエリアPA1のデータをフラッシュメモリのプロテクトエリアPAからの読み出し以外を禁止するように制御する。たとえば、ユーザがアクセス可能なユーザアクセスエリアからプロテクトエリアPAのデータを読み出す場合には、バスステートコントローラ3から、H'FFFFなどの無意味なデータがデータバスを介して出力される。

WO 2006/040798 A1



LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ,  
NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD,  
SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG,  
US, UZ, VC, VN, YU, ZA, ZM, ZW.

IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF,  
BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN,  
TD, TG).

- (84) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE,

添付公開書類:

— 国際調査報告書

2文字コード及び他の略語については、定期発行される各PCTガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

## 明 細 書

### 半導体集積回路装置および電子システム

#### 技術分野

- [0001] 本発明は、不揮発性半導体メモリにおけるデータ保護技術に関し、特に、不揮発性半導体メモリを内蔵した半導体集積回路装置におけるプログラムのコピー、書き換えの防止に適用して有効な技術に関するものである。

#### 背景技術

- [0002] 近年、電子機器の開発・改善の期間短縮を図るため、制御用のプログラムやデータの書き換えが容易な不揮発性半導体メモリを内蔵した半導体集積回路装置、いわゆるフラッシュメモリ内蔵マイクロコンピュータに対するニーズが高まっている。
- [0003] このフラッシュメモリ内蔵マイクロコンピュータには、機密保持のためフラッシュメモリに格納されたアプリケーションプログラムなどの書き換えなどを禁止するプロテクト機能を有するものがある。
- [0004] この種の不揮発性半導体メモリに格納されたデータやプログラムなどの保護機能としては、たとえば、EPROM(Erasable Programmable Read Only Memory)において、プログラマが設定した保護ブロックにプログラムを格納した後、該EPROM内の保護レジスタの指定ビットを設定することによって保護エリア外からの読み出し／書き込みを不可とする技術がある(たとえば、特許文献1参照)。

特許文献1:特開2000-76133号公報

#### 発明の開示

#### 発明が解決しようとする課題

- [0005] ところが、上記のようなフラッシュメモリ内蔵のマイクロコンピュータにおけるプロテクト技術では、次のような問題点があることが本発明者により見い出された。
- [0006] フラッシュメモリのプロテクト機能を有効にした場合には、第三者がアプリケーションプログラムなどを読み出すことはできないが、該フラッシュメモリのすべてメモリ領域(ブロック)にプロテクトがかかってしまうことになるので、ユーザデータなどの書き換えもできなくなってしまうことになる。

- [0007] また、フラッシュメモリは、ブートモードを起動させることによって、電子システムなどのプリント配線基板に実装した状態でアプリケーションプログラムなどの書き換えを容易に行うことができ、第三者によって該アプリケーションプログラムの読み出しや書き換えなどが行われてしまう恐れがある。
- [0008] さらに、フラッシュメモリにプロテクトをかけた状態であっても、マイクロコンピュータに設けられたCPUのワークエリアとして用いられるRAM(Random Access Memory)の内容を読み出し、どのような命令を実行しているかなどを解析することによってアプリケーションプログラムの内容が推測されてしまう恐れがある。
- [0009] 本発明の目的は、不揮発性半導体メモリの特定のメモリ領域における読み出しを禁止することにより、第三者によるプログラムの不正コピーや改ざんなどを確実に防止することのできる技術を提供することにある。
- [0010] 本発明の前記ならびにその他の目的と新規な特徴は、本明細書の記述および添付図面から明らかになるであろう。

#### 課題を解決するための手段

- [0011] 本願において開示される発明のうち、代表的なものの概要を簡単に説明すれば、次のとおりである。
- [0012] 本発明は、複数の不揮発性メモリセルを有するメモリアレイ部と、該不揮発性メモリセルに情報を格納する書き込み動作、該不揮発性メモリセルに格納した情報を読み出す読み出し動作、該不揮発性メモリセルに格納した情報を消去する消去動作の各動作を制御する制御部とを備えた不揮発性記憶部と、該不揮発性記憶部に格納されたプログラムのワークエリアとして用いられる揮発性記憶部と、所定の処理を実行し、該不揮発性記憶部に動作指示を行うことが可能である中央処理装置と、不揮発性記憶部、および揮発性記憶部の読み出し動作を制御するプロテクト動作制御部とを有した半導体集積回路装置であって、メモリアレイ部は、プロテクト動作制御部の制御により格納された情報の読み出しおよび書き込みが禁止される第1のプロテクトメモリ領域を有し、揮発性記憶部は、プロテクト動作制御部の制御によりメモリアレイ部の第1のプロテクトメモリ領域以外からの読み出しおよび書き込みが禁止される第2のプロテクトメモリ領域を有し、不揮発性記憶部の第1のプロテクトメモリ領域に格納された

プログラムのワークエリアとして揮発性記憶部の第2のプロテクトメモリ領域を用いることを特徴とする半導体集積回路装置。

[0013] また、本発明の半導体集積回路装置は、複数の不揮発性メモリセルを有するメモリアレイ部と、該不揮発性メモリセルに情報を格納する書き込み動作、該不揮発性メモリセルに格納した情報を読み出す読み出し動作、該不揮発性メモリセルに格納した情報を消去する消去動作の各動作を制御する制御部とを備えた不揮発性記憶部と、揮発性記憶部と、所定の処理を実行し、該不揮発性記憶部に動作指示を行うことが可能である中央処理装置と、不揮発性記憶部、および揮発性記憶部の読み出し動作を制御するプロテクト動作制御部とを有した半導体集積回路装置であって、メモリアレイ部は、プロテクト動作制御部の制御により格納された情報の読み出しおよび書き込みが禁止される第1のプロテクトメモリ領域を有し、揮発性記憶部は、プロテクト動作制御部の制御によりメモリアレイ部の第1のプロテクトメモリ領域以外からの読み出しおよび書き込みが禁止される第2のプロテクトメモリ領域を有したものである。

[0014] また、本願のその他の発明の概要を簡単に示す。

[0015] 本発明は、複数の不揮発性メモリセルを有するメモリアレイ部と、該不揮発性メモリセルに情報を格納する書き込み動作、該不揮発性メモリセルに格納した情報を読み出す読み出し動作、該不揮発性メモリセルに格納した情報を消去する消去動作の各動作を制御する制御部とを備えた不揮発性半導体記憶装置と、該不揮発性半導体記憶装置に格納されたプログラムのワークエリアとして用いられる揮発性半導体記憶装置と、所定の処理を実行し、不揮発性半導体記憶装置に動作指示を行うことが可能である中央処理装置と不揮発性半導体記憶装置、および揮発性半導体記憶装置の読み出し動作を制御するプロテクト動作制御部とを備えた半導体集積回路装置とを有した電子システムであって、メモリアレイ部は、プロテクト動作制御部の制御により格納された情報の読み出しが禁止される第1のプロテクトメモリ領域を有し、揮発性半導体記憶装置は、プロテクト動作制御部の制御によりメモリアレイ部の第1のプロテクトメモリ領域以外からの読み出しが禁止される第2のプロテクトメモリ領域を有し、不揮発性半導体記憶装置に格納されたプログラムのワークエリアとして第2のプロテクトメモリ領域を用いるものである。

## 発明の効果

- [0016] 本願において開示される発明のうち、代表的なものによって得られる効果を簡単に説明すれば以下のとおりである。
- [0017] (1)第1のプロテクトメモリ領域の読み出しや書き換えなどを制限することができるので、プログラムの不正なコピーや改ざんなどを防止することができ、セキュリティを向上させることができる。
- [0018] (2)また、第2のプロテクトメモリ領域の読み出しを制限することにより、プログラムの推測などを困難にすることが可能となり、プログラムの不正なコピーや改ざんなどをより効果的に防止することができる。
- [0019] (3)上記(1)、(2)により、半導体集積回路装置やそれを用いた電子システムなどの信頼性を大幅に向上させることができる。

## 図面の簡単な説明

- [0020] [図1]本発明の実施の形態1による半導体集積回路装置のブロック図である。
- [図2]図1の半導体集積回路装置に設けられたフラッシュメモリにおけるメモリマップの一例を示した説明図である。
- [図3]図1の半導体集積回路装置に設けられたRAMにおけるメモリマップの一例を示した説明図である。
- [図4]図1の半導体集積回路装置に設けられたバスステートコントローラの一部構成例を示した説明図である。
- [図5]図1の半導体集積回路装置に設けられたフラッシュメモリにおける消去禁止制御回路、および書き換え禁止制御回路のブロック図である。
- [図6]図1の半導体集積回路装置に設けられたフラッシュメモリのユーザアクセスエリアにおける読み出し制御動作例を示すタイミングチャートである。
- [図7]図1の半導体集積回路装置に設けられたフラッシュメモリのユーザアクセスエリアからプロテクトエリアを読み出す場合の制御動作例を示すタイミングチャートである。
- 。
- [図8]図1の半導体集積回路装置に設けられたフラッシュメモリのプロテクトエリアからプロテクトエリアを読み出す場合の制御動作例を示すタイミングチャートである。

[図9]図1の半導体集積回路装置に設けられたフラッシュメモリのプロテクトエリアからRAMのプロテクトエリアのデータを読み出す場合の制御動作例を示すタイミングチャートである。

[図10]図1の半導体集積回路装置に設けられたRAMの処理例を示した説明図である。

[図11]図1の半導体集積回路装置における第一ユーザによるキーコードの設定例を示すフローチャートである。

[図12]図1の半導体集積回路装置におけるエンドユーザによるキーコードの設定例を示すフローチャートである。

[図13]本発明の実施の形態2による半導体集積回路装置のブロック図である。

[図14]図13の半導体集積回路装置におけるリセットシーケンスを示した説明図である。

[図15]図14のリセットシーケンスにおけるプロテクト処理制御部の設定処理を示すフローチャートである。

[図16]図13の半導体集積回路装置に設けられたフラッシュメモリにおけるプロテクトエリアの任意設定処理を示すフローチャートである。

[図17]図16におけるフラッシュメモリのメモリマップの補足説明図である。

### 発明を実施するための最良の形態

[0021] 以下、本発明の実施の形態を図面に基づいて詳細に説明する。なお、実施の形態を説明するための全図において、同一の部材には原則として同一の符号を付し、その繰り返しの説明は省略する。

[0022] (実施の形態1)

図1は、本発明の実施の形態1による半導体集積回路装置のブロック図、図2は、図1の半導体集積回路装置に設けられたフラッシュメモリにおけるメモリマップの一例を示した説明図、図3は、図1の半導体集積回路装置に設けられたRAMにおけるメモリマップの一例を示した説明図、図4は、図1の半導体集積回路装置に設けられたバスステートコントローラの一部構成例を示した説明図、図5は、図1の半導体集積回路装置に設けられたフラッシュメモリにおける消去禁止制御回路、および書き換え禁

止制御回路のブロック図、図6は、図1の半導体集積回路装置に設けられたフラッシュメモリのユーザアクセスエリアにおける読み出し制御動作例を示すタイミングチャート、図7は、図1の半導体集積回路装置に設けられたフラッシュメモリのユーザアクセスエリアからプロテクトエリアを読み出す場合の制御動作例を示すタイミングチャート、図8は、図1の半導体集積回路装置に設けられたフラッシュメモリのプロテクトエリアからプロテクトエリアを読み出す場合の制御動作例を示すタイミングチャート、図9は、図1の半導体集積回路装置に設けられたフラッシュメモリのプロテクトエリアからRAMのプロテクトエリアのデータを読み出す場合の制御動作例を示すタイミングチャート、図10は、図1の半導体集積回路装置に設けられたRAMの処理例を示した説明図、図11は、図1の半導体集積回路装置における第一ユーザによるキーコードの設定例を示すフローチャート、図12は、図1の半導体集積回路装置におけるエンドユーザによるキーコードの設定例を示すフローチャートである。

- [0023] 本実施の形態1において、半導体集積回路装置1は、図1に示すように、CPU(中央処理装置)2、バスステートコントローラ(プロテクト動作制御部)3、RAM(揮発性記憶部)4、SCI(Serial Communication Interface)5などを含む周辺回路6、およびフラッシュメモリ7に例示される不揮発性半導体メモリなどから構成されている。
- [0024] CPU2は、フラッシュメモリ(不揮発性記憶部)7に格納された命令を読み出し、所定の処理を行う。バスステートコントローラ3は、アドレスバスやデータバスなどを含む内部バスBにおける信号の転送を制御するとともに、該内部バスBの状態を制御する。RAM(揮発性メモリ)4は、随時読み出し／書き込みが可能なメモリであり、CPU2のワークエリアとして用いられる。
- [0025] SCI5は、外部接続されるデバイスとシリアル通信を行うインタフェースである。周辺回路6は、そのほかに、たとえば、タイマ、WDT(Watch Dog Timer)、TPU(Timer Pulse Unit)、A/D(Analog/Digital)変換器、およびD/A(Digital/Analog)変換器などから構成されている。
- [0026] タイマは、たとえば、8ビットのカウンタをベースとしたタイマである。WDTは、半導体集積回路装置1の暴走などの監視を行う。TPUは、PWM(Pulse Width Modulation)波形を出力することのできるタイマである。A/D変換器は、アナログ信号を



デジタル信号に変換して出力する。D/A変換器は、デジタル信号をアナログ信号に変換して出力する。

- [0027] フラッシュメモリ7は、電氣的にデータの書き換え／消去が可能な不揮発性半導体メモリであり、CPU2によって実行されるプログラム命令を含む制御プログラムなどを格納する。フラッシュメモリ7は、CPU2からの指示に応じてデータの書き込み／読み出しや消去などを行う。
- [0028] これらCPU2、バスステートコントローラ3、RAM4、SCI5などを含む周辺回路6、およびフラッシュメモリ7は、内部バスBにより相互に接続されている。
- [0029] また、CPU2からは、次に読み出される命令のアドレスを示すプログラムカウンタの値、書き込みを許可するライト信号、ならびに読み出しを許可するリード信号がバスステートコントローラ3に入力されるように接続されている。
- [0030] RAM4には、バスステートコントローラ3から出力されたRAMセレクト信号S1、ライト信号、およびリード信号がそれぞれ入力されるように接続されている。RAMセレクト信号S1は、RAM4を選択する信号である。ライト信号は、RAM4のライトを許可する信号であり、リード信号はRAM4のリードを許可する信号である。
- [0031] SCI5には、シリアルセレクト信号、ライト信号、ならびにリード信号がそれぞれ入力されるように接続されている。シリアルセレクト信号は、SCI5を選択する信号である。ライト信号は、SCI5のライトを許可する信号であり、リード信号はSCI5のリードを許可する信号である。
- [0032] フラッシュメモリ7には、フラッシュメモリセレクト信号、ライト信号、およびリード信号がそれぞれ入力されるように接続されている。フラッシュメモリセレクト信号は、フラッシュメモリ7を選択する信号である。ライト信号は、フラッシュメモリ7のライトを許可する信号であり、リード信号は該フラッシュメモリ7のリードを許可する信号である。
- [0033] フラッシュメモリ7は、メモリマツト(メモリアレイ部)7a、および制御回路(制御部)7bから構成されている。
- [0034] メモリマツト7aは、記憶の最小単位であるメモリセルが規則正しくアレイ状に並べられており、アドレスバッファ、行デコーダ、列デコーダ、およびセンスアンプなどの周辺回路を含んでいる。制御回路7bは、CPU2から入力される各種制御用信号を一時

的に格納し、動作ロジックの制御を行う。

[0035] 図2は、フラッシュメモリ7のメモリマップ7aにおけるメモリマップの一例を示した説明図である。

[0036] 図示するように、メモリマップ7a、ユーザアクセスエリアUAとプロテクトエリア(第1のプロテクトメモリ領域)PAとから構成されている。ユーザアクセスエリアUAは、ユーザがアクセスできる複数の領域(ブロック)から構成されている。また、プロテクトエリアPAは、プログラムやデータなどが格納された領域(ブロック)であり、これらプログラムやデータなどの読み出しが制限される。プロテクトエリアPAは一つの連続したアドレス領域のみに限られず、例えば、複数の領域に配置されていてもよい。

[0037] 図3は、RAM4におけるメモリマップの一例を示した説明図である。

[0038] RAM4においても同様に、ユーザアクセスエリアUA1とプロテクトエリア(第2のプロテクトメモリ領域)PA1とから構成されている。ユーザアクセスエリアUA1は、フラッシュメモリ7などのデータを展開する領域であり、プロテクトエリアPA1は、フラッシュメモリ7のプロテクトエリアPA(第1のプロテクトメモリ領域)に格納されたプログラムのワークエリアとして用いられる領域である。

[0039] メモリマップ7aのプロテクトエリアPAに格納されているプログラムやデータは、該プロテクトエリアPA内のプログラムによって読み出すことは可能となっているが、該メモリマップ7aのユーザアクセスエリアUAやRAM4のユーザアクセスエリアUA1やプロテクトエリアPA1に格納されたプログラムからの読み出しは不可となっている。

[0040] また、RAM4のプロテクトエリアPA1に格納されているデータなどは、メモリマップ7aのプロテクトエリアPAから読み出すことは可能であるが、そのほかのエリア(メモリマップ7aのユーザアクセスエリアUA、およびRAM4のユーザアクセスエリアUA、プロテクトエリアPA1)からの読み出しは不可となっている。

[0041] さらに、フラッシュメモリ7は、後述するキーコードエリアKA(図5)に所定のキーコードを設定するまでは、フラッシュメモリ7のプロテクトエリアPAにプログラムやデータなどをRAM4のユーザアクセスエリアUA1から書き換え／消去することが可能となっている。所定のキーコードを設定するまでは、フラッシュメモリ7のプロテクトエリアPAやユーザアクセスエリアUAやユーザアクセスエリアUA1、何れの領域からもそれぞれ

の領域に対してアクセスが可能となる。

- [0042] キーコードが設定された場合には、フラッシュメモリ7のプロテクトエリアPAを書き換え／消去することが不可となる。
- [0043] RAM4のプロテクトエリアPA1に格納されているデータなどは、フラッシュメモリ7のプロテクトエリアPAから書き換え／消去することが可能となっているが、そのほかのエリア(フラッシュメモリ7のユーザアクセスエリアUA、RAM4のユーザアクセスエリアUA1、プロテクトエリアPA1)からの書き換え／消去は不可となっている。更に、キーコードの設定有無に関わらずRAMのプロテクトエリアPA1は、プロテクト動作制御部の制御によってフラッシュメモリ7のプロテクトエリアPA以外からの書き換え／消去が禁止される。
- [0044] また、フラッシュメモリ7において、読み出しが禁止されているプロテクトエリアPAのプログラムやデータなどをユーザアクセスエリアUAから読み出した場合には、たとえば、常にH'FFのデータが読み出される。
- [0045] ここでは、フラッシュメモリ7に書き込まれている初期値のデータにあわせてH'FFとしたが、この場合に読み出されるデータは、ハイインピーダンス状態(Hi-Z)以外であればよく、たとえば、H'00や前値保持などの無意味なデータ、ユーザが設定した任意の値などであってもよい。
- [0046] 同様に、RAM4において、読み出しが禁止されているプロテクトエリアPA1のプログラムやデータなどをユーザアクセスエリアUA1から読み出した場合には、たとえば、常にH'00のデータが読み出される。
- [0047] ここでも、RAM4のNOP命令にあわせてH'00としたが、読み出されるデータは、ハイインピーダンス状態(Hi-Z)以外であればよく、たとえば、H'FFや前値保持などの無意味なデータ、ユーザが設定した任意の値などであってもよい。
- [0048] 図4は、バスステートコントローラ3の一部構成例を示した説明図である。
- [0049] バスステートコントローラ3は、図示するように、セクタ8〜11、否定論理和回路12、13、およびドライバ14、15などから構成されている。
- [0050] セクタ8〜11の一方の入力部には、CPU2(図1)から出力されるアドレス信号が入力されるようにそれぞれ接続されており、該セクタ8〜11の他方の入力部には、

CPU2から出力されるプログラムカウンタ値(PC値)が入力されるようにそれぞれ接続されている。

[0051] セレクタ8は、アドレス信号が、フラッシュメモリ7のユーザアクセスエリアUA(図2)を示すアドレスH'00\_0000〜H'00\_FFFF、またはアドレスH'02\_0000〜H'03\_FFFF、あるいはフラッシュメモリ7のプロテクトエリアPA(図2)を示すアドレスH'01\_0000〜H'01\_FFFF、かつプログラムカウンタの値が、H'01\_0000〜01\_FFFFとなった場合にフラッシュメモリセレクト信号がアクティブとなる'0'(Loレベル信号)を出力し、そのほかの場合には、該フラッシュメモリセレクト信号がインアクティブとなる'1'(Hiレベル信号)を出力する。つまり、CPU2が出力するアドレス値がフラッシュメモリ7のユーザアクセスエリアUAを示す場合はプログラムカウンタ値によらずアクセスが可能である。更に、アドレス値がフラッシュメモリ7のプロテクトエリアPAを示し、かつプログラムカウンタの値もフラッシュメモリ7のプロテクトエリアPAを示す場合、フラッシュメモリ7はアクセス可能な状態、つまりセレクト信号がアクティブ状態となる。

[0052] セレクタ9は、アドレス信号が、RAM4のユーザアクセスエリアUA1(図3)を示すアドレスH'FF\_D800〜H'FF\_EFFF、またはRAM4のプロテクトエリアPA1(図3)を示すアドレスH'FF\_D000〜H'FF\_D7FF、かつプログラムカウンタの値が、H'01\_0000〜01\_FFFF(フラッシュメモリ7のプロテクトエリアPAを示すアドレス)となった場合にRAMセレクト信号がアクティブとなる'0'(Loレベル信号)を出力し、そのほかの場合には、該RAMセレクト信号がインアクティブとなる'1'(Hiレベル信号)を出力する。つまり、CPU2が出力するアドレス値がRAM4のユーザアクセスエリアUA1を示す場合はプログラムカウンタ値によらずアクセスが可能である。更に、プログラムカウンタ値がフラッシュメモリ7のプロテクトエリアPAを示し、アドレス値がRAM4のプロテクトエリアPA1を示す場合は、RAM4はアクセス可能な状態となる。

[0053] セレクタ10は、アドレス信号が、フラッシュメモリ7のプロテクトエリアPAを示すアドレスH'01\_0000〜H'01\_FFFF、かつプログラムカウンタの値がH'01\_0000〜01\_FFFF以外となった場合に、'0'の信号を出力し、アドレスH'01\_0000〜H'01\_FFFF、かつプログラムカウンタの値がH'01\_0000〜01\_FFFFの場合に

は、'1'の信号を出力する。

[0054] セクタ11は、アドレス信号が、RAM4のプロテクトエリアPA1を示すアドレスH'FF\_D000〜H'FF\_D7FF、かつプログラムカウンタの値がH'01\_0000〜01\_FFFF以外となった場合に、'0'の信号を出力し、アドレス値がH'FF\_D000〜H'FF\_D7FF、かつプログラムカウンタの値がH'01\_0000〜01\_FFFFの場合には、'1'の信号を出力する。

[0055] このように、フラッシュメモリ7のプロテクトエリアPAをリード／ライトする際のフラッシュメモリ7のセレクト条件としては、プログラムカウンタの値とアドレス信号の値とが、いずれもフラッシュメモリ7のプロテクトエリアPAに一致する場合にのみ、フラッシュメモリセレクト信号が有効になる。上記一致する場合以外はフラッシュメモリセレクト信号は無効となる。

[0056] RAM4においても、該RAM4のプロテクトエリアPA1をリード／ライトする場合のRAM4のセレクト条件としては、プログラムカウンタの値がフラッシュメモリ7のプロテクトエリアPAで、かつアドレス値がRAM4のプロテクトエリアPA1である場合に限ってRAMセレクト信号が有効となる。上記の場合以外にはRAMセレクト信号は無効となる。

[0057] 否定論理和回路12は、セクタ10から出力される信号とリード信号との否定論理和をとり、ドライバ14の制御部に出力する。否定論理和回路12は、アドレス信号が、フラッシュメモリ7のプロテクトエリアPAを示すアドレスH'01\_0000〜H'01\_FFFF、かつプログラムカウンタの値がH'01\_0000〜01\_FFFF以外となり、かつアクティブなリード信号('0')が入力された際にドライバ14からフラッシュメモリ7の初期値であるH'FFFFが出力されるように制御信号を出力する。上記制御に従い、内部バスBのデータ信号にはH'FFFFが出力される。ここで、出力される信号の値はH'FFFFに限られず、出力値を任意に設定することも可能である。つまりCPU2が出力するアドレス信号に従ったフラッシュメモリ7からの読み出しデータでない限り、どのような値が出力可能な構成であってもよい。

[0058] 否定論理和回路13は、セクタ11から出力される信号とリード信号との否定論理和をとりドライバ15の制御部に出力する。否定論理和回路13は、アドレス信号が、R

AM4のプロテクトエリアPA1を示すアドレスH'FF\_D000〜H'FF\_D7FF、かつプログラムカウンタの値がH'01\_0000〜H'01\_FFFF以外となり、かつアクティブなリード信号('0')が入力された際にドライバ15からRAM4のNOP命令にあわせた値であるH'0000が出力されるように制御信号を出力する。上記制御に従い、内部バスBのデータ信号にはH'0000が出力される。ここで、出力される信号の値はH'0000に限られず、出力値を任意に設定することも可能である。つまりCPU2が出力するアドレス信号に従ったRAM4からの読み出しデータでない限り、どのような値が出力可能な構成であってもよい。

[0059] ここで、CPU2からフラッシュメモリ7、または'0')が出力された場合で、上記フラッシュメモリセレクト信号RAMセレクト信号が無効である場合にはフラッシュメモリ7およびRAM4へのアクセスが禁止されるため、データ信号は、たとえば前値保持の状態となる。

[0060] 図5は、フラッシュメモリ7における該フラッシュメモリ7の動作制御を司る制御回路7bに設けられた消去禁止制御回路(消去禁止制御部)16、ならびに書き換え禁止制御回路(書き換え禁止制御部)17のブロック図である。

[0061] 消去禁止制御回路16は、フラッシュメモリ7の消去禁止を制御する回路であり、予めメモリマツト7aのキーコードエリアKAに書き込まれたキーコード(第1の設定値)が予め設定されているキーコード(第2の設定値)と一致した場合、メモリマツト7aのプロテクトエリアPAに対するデータへの消去が発生した際に該プロテクトエリアPAの消去を禁止する。

[0062] 消去禁止制御回路16は、キーコード発生部(キーコード発生回路)18、排他的否定論理和回路(消去制御回路)19、および論理積回路(消去制御回路)20から構成されている。キーコード発生部18は、予め設定するキーコード(第2の設定値、たとえば、H'1234)をハードウェアによって出力する回路からなる。

[0063] 排他的否定論理和回路19の一方の入力部には、キーコード発生部18が生成したキーコード(H'1234)が入力されるように接続されており、該排他的否定論理和回路19他方の入力部には、キーコードエリアKAに格納されているキーコード(第1の設定値)が入力されるように接続されている。

- [0064] 論理積回路20の一方の入力部には、イレースブロックセクタEBSから出力されるイレースブロック信号EB9が入力されるように接続されている。イレースブロックセクタEBSは制御回路7bに設けられており、どのブロックを消去するかを選択するレジスタのうちの1つである。このイレースブロックセクタEBSは、フラッシュメモリ7のメモリマツト7aにおけるプロテクトエリアPA(Block9)を消去する際に'0'のイレースブロック信号EB9を出力する。
- [0065] 論理積回路20の他方の入力部には、排他的否定論理和回路19から出力される信号が入力されるように接続されている。論理積回路20の出力部には、フラッシュメモリ7の読み出し／書き込みを制御する読み出し／書き込み制御回路30の入力部が接続されており、論理積回路20の出力部からイレースブロック制御信号EBC9が出力される。
- [0066] 上記キーコード発生部18が生成したキーコード(第2の設定値)がキーコードエリアに格納されているキーコード(第1の設定値)に一致する場合、上記消去禁止制御回路16はイレースブロック制御信号が無効となるように制御し、上記読み出し／書き込み制御回路30は消去動作を禁止する。
- [0067] 上記イレースブロック制御信号EBC9が有効な状態の時、上記読み出し／書き込み制御回路30はプロテクトエリアPA(Block9)に対する消去制御を行う。
- [0068] ここで、フラッシュメモリ7のメモリセル部に複数のプロテクトエリアを設置する場合には、プロテクトエリア毎に上記消去禁止制御回路16を用意すればよい。これにより複数のプロテクトエリアに対する消去制御が可能となる。
- [0069] また、書き換え禁止制御回路17は、キーコード発生部(キーコード発生回路)21、アドレス判定部(アドレス判定回路)22、排他的否定論理和回路(キーコード判定部)23、インバータ(書き換え制御回路)24〜26、否定論理積回路(書き換え制御回路)27、保持回路(書き換え制御回路)28、および論理積回路(書き換え制御回路)29から構成されている。
- [0070] キーコード発生部21は、予め設定するキーコード(第3の設定値、たとえば、H'1234)をハードウェアによって出力する回路からなる。排他的否定論理和回路23の一方の入力部には、キーコード発生部18が生成したキーコード(H'1234)が入力され

るように接続されており、該排他的否定論理和回路23の他方の入力部には、キーコードエリアKAに格納されているキーコード(第1の設定値)が入力されるように接続されている。

- [0071] アドレス判定部22には、アドレス信号が入力されており、該アドレス判定部22は、アドレス信号がアドレスH'01\_0000〜H'01\_FFFFの場合には、'0'を出力し、それ以外の場合には'1'を出力する。
- [0072] インバータ24〜26の入力部には、メモリセレクト信号(図1)、ライト信号(図1)、およびアドレス判定部22から出力される判定信号がそれぞれ入力されるように接続されている。
- [0073] 否定論理積回路27の入力部には、排他的否定論理和回路23の出力部、インバータ24〜26の出力部がそれぞれ接続されており、該否定論理積回路27の出力部には、保持回路28の入力部が接続されている。この保持回路28は、フラッシュメモリ7への書き込みが発生するまで、その信号状態を保持する回路である。
- [0074] 論理積回路29の一方の入力部には、プログラミングビットPBから出力されるプログラムモード信号Pが入力されるように接続されている。プログラミングビットPBは、書き換えを開始するプログラムモードを解除／遷移させるビットであり、'0'の際にはプログラムモードが解除となり、'1'の場合にはプログラムモードに遷移する。
- [0075] 論理積回路29の出力部には、読み出し／書き込み制御回路30の入力部が接続されており、論理積回路29の出力部からプログラムモード信号Pが出力される。
- [0076] 上記キーコード発生部21が生成したキーコード(第3の設定値)がキーコードエリアに格納されているキーコード(第1の設定値)に一致する場合、上記読み出し／書き込み制御回路30は書き換え動作を禁止する。
- [0077] 上記プログラムモード信号Pが有効な状態の時、上記読み出し／書き込み制御回路30はプロテクトエリアPA(Block9)に対する書き換え制御を行う。
- [0078] ここでは、キーコードをH'1234としたが、該キーコードは、フラッシュメモリ7に格納されている初期値(H'FFFF)以外であれば、どのようなデータでもよい。
- [0079] 次に、本実施の形態における半導体集積回路装置1の作用について説明する。
- [0080] 図6から図9に示されるCPU2によって実行される命令は一つの具体例であって、



それだけに限られず、各種の命令が実行される。アドレスに対応したメモリに格納されている命令やデータの値(たとえば、図6のアドレスH'00\_\_4008には「H'6828」が格納される)もプログラムによって様々である。本発明ではバスステートコントローラ3によるアドレス値およびプログラムカウンタの値の比較によって各種メモリおよびその他の周辺回路に対するアクセスが制御されるものである。

- [0081] 始めに、フラッシュメモリ7のユーザアクセスエリアUAにおける読み出し制御動作について、図6を用いて説明する。
- [0082] 図6の上方は、フラッシュメモリ7による読み出し制御の説明図を示しており、その下方には、各部信号のタイミングチャートを示している。
- [0083] この図6のタイミングチャートにおいては、上方から下方にかけて、クロック信号 $\phi$ 、CPU2から出力されるプログラムカウンタの値、CPU2から出力されるアドレス信号、バスステートコントローラ3から出力されるフラッシュメモリセレクト信号、CPU2から出力されるデータ信号、およびプログラムカウンタの値がフラッシュメモリ7のプロテクトエリアPAを示しているか否かを示す状態信号(PC=H'01\_\_xxxx)をそれぞれ示している。
- [0084] まず、CPU2のプログラムカウンタは、アドレスH'00\_\_4000番地を示し、アドレスH'00\_\_4000を内部バスに出力し、アドレスH'00\_\_4000番地における命令をCPU2がメモリから順次読み出す。続いて、CPU2は、汎用レジスタ(E2)にH'0000を格納する。
- [0085] その後、CPU2は、アドレスH'00\_\_4004番地の命令を読み出し、続いて、アドレスH'00\_\_4006を読み出して、汎用レジスタ(R2)にH'0C00を格納する。
- [0086] そして、CPU2は、アドレスH'00\_\_4008の命令を読み出して、該命令を解析(汎用レジスタER2が示すアドレス値が示すメモリに格納されているデータをリード)した後、その命令を実行してアドレスH'00\_\_0C00のデータを読み出し、汎用レジスタ(R0L)にH'1234を格納する。
- [0087] この場合、フラッシュメモリ7におけるプロテクトエリアPAの読み出しがない、つまりアドレス値がプロテクトエリアPAを示さないため、制限なくプログラム／データなどを読み出すことができる。

- [0088] また、フラッシュメモリ7のユーザアクセスエリアUAからプロテクトエリアPAを読み出す場合の制御動作について、図7を用いて説明する。
- [0089] この図7においても、上方に、フラッシュメモリ7による読み出し制御の説明図を示しており、その下方に、各部信号のタイミングチャートを示している。タイミングチャートは、上方から下方にかけて、クロック信号 $\phi$ 、CPU2から出力されるプログラムカウンタの値、CPU2から出力されるアドレス信号、バスステートコントローラ3から出力されるフラッシュメモリセレクト信号、データ、およびプログラムカウンタがフラッシュメモリ7のプロテクトエリアPAか否かを示す状態信号(PC=H'01\_XXXX?)をそれぞれ示している。
- [0090] まず、CPU2のプログラムカウンタが、アドレスH'00\_400Aを示し、内部バスにアドレスH'00\_400Aを出力し、アドレスH'00\_400A番地の命令をメモリから順次読み出し、汎用レジスタ(E2)にH'0001を格納する。その後、CPU2は、アドレスH'00\_400E、およびアドレスH'00\_4010番地を順次読み出して、汎用レジスタ(R2)にH'0000を格納する。その後、CPU2は、アドレスH'00\_4012の命令を読み出して解析(汎用レジスタER2が示すアドレス値が示すメモリに格納されているデータをリード)を行い、それに基づいて、CPU2は、アドレスH'01\_0000のデータを読み出す。
- [0091] このとき、アドレスH'01\_0000は、フラッシュメモリ7のプロテクトエリアPA内であり、かつCPU2から出力されるプログラムカウンタの値がプロテクトエリアPA外(ここではH'00\_4014)となっているので、バスステートコントローラ3から出力されるフラッシュメモリセレクト信号がインアクティブ('1')となり、バスステートコントローラ3の制御により、内部バスBのアドレス信号には、H'FFFFのデータが出力されることになる。
- [0092] 上記構成により、ユーザエリアUAからプロテクトエリアPAに対するデータ読み出しアクセスを禁止することが可能となる。
- [0093] さらに、フラッシュメモリ7のプロテクトエリアPAからプロテクトエリアPAを読み出す場合の制御動作について、図8を用いて説明する。
- [0094] 図8も、上方に、フラッシュメモリ7による読み出し制御の説明図を示しており、その下方に、各部信号のタイミングチャートを示している。タイミングチャートは、上方から

下方にかけて、クロック信号 $\phi$ 、CPU2から出力されるプログラムカウンタの値、CPU2から出力されるアドレス信号、バスステートコントローラ3から出力されるフラッシュメモリセレクト信号、データ、およびプログラムカウンタがフラッシュメモリ7のプロテクトエリアPAか否かを示す状態信号(PC=H'01\_XXXX?)をそれぞれ示している。

[0095] まず、CPU2が、アドレスH'01\_0000、およびアドレスH'01\_0002番地に格納される命令を順次読み出し、汎用レジスタ(E2)にH'0001を格納する。その後、CPU2は、アドレスH'01\_0004、アドレスH'01\_0006の命令をそれぞれ読み出して汎用レジスタ(R2)にH'0100を格納する。

[0096] 続いて、CPU2は、アドレスH'01\_0008の命令を読み出して解析(汎用レジスタER2が示すアドレスが示すメモリに格納されているデータをリード)を行い、それに基づいて、CPU2は、命令を実行してアドレスH'01\_0100に格納されるデータを読み出し、汎用レジスタ(R0L)にH'1234を格納する。

[0097] この場合、プロテクトエリアPAからプロテクトエリアPAを読み出すので、プログラムカウンタの値もプロテクトエリアPA内となっており、フラッシュメモリセレクト信号がアクティブ('0')のままとなり、フラッシュメモリ7から読み出された正常なデータが内部バスBのデータ信号(Data)へ出力されることになる。

[0098] 次に、フラッシュメモリ7のプロテクトエリアPAからRAM4のプロテクトエリアPA1のデータを読み出す場合の制御動作について、図9を用いて説明する。

[0099] この図9においては、上方に、フラッシュメモリ7、およびRAM4による読み出し制御の説明図を示しており、その下方に、各部信号のタイミングチャートを示している。タイミングチャートは、上方から下方にかけて、クロック信号 $\phi$ 、CPU2から出力されるプログラムカウンタの値、CPU2から出力されるアドレス信号、同様にバスステートコントローラ3から出力されるRAMメモリセレクト信号、データ、およびプログラムカウンタの値がフラッシュメモリ7のプロテクトエリアPAか否かを示す状態信号(PC=H'01\_XXXX?)をそれぞれ示している。

[0100] まず、CPU2が、アドレスH'01\_5000、およびアドレスH'01\_5002の命令を順次読み出し、汎用レジスタ(E2)にH'FFFFを格納する。その後、CPU2は、アドレスH'01\_5004、ならびにアドレスH'01\_5006の命令を順次読み出し、汎用レジスタ

タ(R2)にH'D000を格納する。

- [0101] その後、CPU2は、アドレスH'01\_5008の命令を読み出し、その命令の解析(汎用レジスタER2が示すアドレスが示すメモリに格納されているデータをリード)を行い、それに基づいて、CPU2は、RAM4におけるアドレスH'FF\_D000のデータを読み出して汎用レジスタ(ROL)に読み出したH'1234を格納する。
- [0102] この場合、プログラムカウンタの値(H'01\_50xx)は、プロテクトエリアPA1にあるので、バスステートコントローラ3から出力されるRAMセレクト信号がアクティブ('0')となり、正常なデータがRAM4から読み出されることになる。
- [0103] ここで、ワークエリアとして用いられるRAM4の処理例について、図10を用いて説明する。
- [0104] この図10では、たとえば、文字データを圧縮する場合の手順について説明する。図10の左側は、RAM4とフラッシュメモリ7との説明図であり、右側は、処理手順のフローチャートである。
- [0105] まず、文字データをRAM4上に展開し(ステップS101)、RAM4のプロテクトエリアPA1へサブルーチンジャンプする(ステップS102)。その後、プロテクトエリアPAに格納されたプログラムに基づく圧縮処理において、圧縮処理の中間データ、圧縮処理結果をプロテクトエリアPA1に格納する(ステップS103)。
- [0106] 続いて、プロテクトエリアPAに格納されたプログラムに基づく暗号化処理において、暗号化処理の中間データ、暗号化結果をプロテクトエリアPA1に格納し(ステップS104)、暗号化結果データをユーザアクセスエリアUA1に格納する(ステップS105)。
- [0107] その後、リターンサブルーチンにより(ステップS106)、暗号化結果データを、たとえば半導体集積回路装置1に外部接続された外部メモリに格納する(ステップS107)。
- [0108] このように、圧縮、暗号化のプログラム処理をRAM4のPプロテクトエリアPA1で処理することによって、該プログラムがどのような処理を行っているかを推測しにくくすることができる。
- [0109] 次に、図5に示す制御回路7bに設けられた消去禁止制御回路16、および書き換え禁止制御回路17の動作について説明する。

- [0110] まず、フラッシュメモリ7の消去動作において、プロテクトエリアPAのブロック(Block 9)が指定されると、イレースブロックセクタEBSから、'0'のイレースブロック信号EB9が出力される。
- [0111] このとき、消去禁止制御回路16は、キーコードエリアKAに格納されているキーコード(第1の設定値)を読み出し、排他的否定論理和回路19によって、読み出した該キーコードとキーコード発生部18が生成したキーコード(第2の設定値)との排他的否定論理和をとり、読み出したキーコードとキーコード発生部18が生成したキーコードとが一致した際に、後段の論理積回路20から、'0'のイレースブロック制御信号EBC9が読み出し／書き込み制御回路30に出力される。このイレースブロック制御信号EBC9によって、フラッシュメモリ7における消去動作が禁止されることになる。
- [0112] また、フラッシュメモリ7の書き換え動作では、まず、プログラミングビットPBから、'1'のプログラムモード信号Pが出力され、書き換え先を指定するアドレスが入力される。
- [0113] アドレス判定部22は、入力されたアドレス信号がプロテクトエリアPA内か否かを判定する。また、排他的否定論理和回路19では、キーコード発生部21が生成したキーコード(第3の設定値)とキーコードエリアKAに格納されているキーコード(第1の設定値)とを比較し、一致している際には'0'の信号を出力する。
- [0114] さらに、フラッシュメモリ7の書き換えであるので、それぞれアクティブ('0')のフラッシュメモリセレクト信号、およびライト信号がバスステートコントローラ3から出力されている。
- [0115] このとき、入力されたアドレスがプロテクトエリアPA内の場合には、アドレス判定部22から、'0'の信号が出力され、保持回路28を介して、'0'の信号が論理積回路29の他方の入力部に入力される。
- [0116] よって、プログラミングビットPBからは、'1'のプログラムモード信号Pが出力されているので、論理積回路29からは、'0'のプログラムモード信号Pが読み出し／書き込み制御回路30に出力される。これにより、フラッシュメモリ7における書き換え動作が禁止されることになる。
- [0117] また、入力されたアドレスがプロテクトエリアPA外の場合には、アドレス判定部22から、'1'の信号が出力されるので論理積回路29から出力されるプログラムモード信号

Pは、'1'となり、フラッシュメモリ7の書き換えが行われる。

- [0118] 次に、第一ユーザ(たとえば、ソフトIPベンダ)がプログラムを書き込んだ後にエンドユーザに半導体集積回路装置1を出荷し、第一ユーザにおいてキーコードを設定する際の処理について、図11のフローチャートを用いて説明する。
- [0119] まず、第1ユーザが作成したキーとなるプログラム(第1プログラム)のデバッグを開始し(ステップS201)。キーとなるプログラムの書き込みと消去(ステップS202)をデバッグが完了するまで行う(ステップS203)。そして、デバッグが完了すると、キーコードエリアKAにキーコード(第1の設定値)を書き込み(ステップS204)、ユーザアクセスエリアUAに格納されているデバッグ用プログラム(第3プログラム)などを消去してエンドユーザに出荷する(ステップS205)。
- [0120] その後、エンドユーザ側において、エンドユーザが作成したメインプログラム(第2プログラム)のデバッグを開始する(ステップS301)。デバッグにより発生するメインプログラムの書き込み／消去をデバッグが終了するまで行う(ステップS302, S303)。
- [0121] これらステップS302, S303の処理では、キーコードが第一ユーザにより設定されているので、エンドユーザによるプロテクトエリアPAに格納されている第一ユーザが書き込んだプログラム(第1プログラム)の書き込み／消去は不可となっている。
- [0122] また、エンドユーザによりキーコードを設定する際の処理について、図12を用いて説明する。
- [0123] まず、エンドユーザにおいて、プロテクトエリアPAに格納されるキーとなるプログラム(第1プログラム)およびユーザエリアに格納されるメインプログラム(第2プログラム)のデバッグを開始する(ステップS401)。そして、デバッグにより発生するキーとなるプログラム(第1プログラム)およびメインプログラム(第2プログラム)の書き込み／消去を行う(ステップS402)。
- [0124] 続いて、デバッグが終了すると(ステップS403)、キーコードエリアにキーコード(第1の設定値)を書き込み、プロテクトエリアPAに書き込まれたキーとなるプログラムを保護する(ステップS404)。
- [0125] それにより、本実施の形態1によれば、キーとなるプログラムに対しプロテクトを行うことが可能であるため、第三者によるキーとなるプログラムの読み出しやコピー、ある

いは変更などを防止することができる。

[0126] (実施の形態2)

図13は、本発明の実施の形態2による半導体集積回路装置のブロック図、図14は、図13の半導体集積回路装置におけるリセットシーケンスを示した説明図、図15は、図14のリセットシーケンスにおけるプロテクト処理制御部の設定処理を示すフローチャート、図16は、図13の半導体集積回路装置に設けられたフラッシュメモリ7におけるプロテクトエリアの任意設定処理を示すフローチャート、図17は、図16におけるフラッシュメモリ7のメモリマップの補足説明図である。

[0127] 本実施の形態2において、半導体集積回路装置1は、図13に示すように、CPU2、バスステートコントローラ3、RAM4、SCI(Serial Communication Interface)5などを含む周辺回路6、およびフラッシュメモリ7に例示される不揮発性半導体メモリなどの前記実施の形態1と同様の構成となっている。

[0128] 前記実施の形態1では、フラッシュメモリ7のプロテクトエリアPAを、アドレスH'01\_0000〜H'01\_FFFFまでの1つのブロックに固定されていたが、本実施の形態2のフラッシュメモリ7では、プロテクトエリアPAの領域を任意に変更することが可能となっている。

[0129] フラッシュメモリ7は、メモリマツト7a、および制御回路7bから構成されており、該メモリマツト7aは、記憶の最小単位であるメモリセルが規則正しくアレイ状に並べられており、アドレスバッファ、アドレスデコーダ7a1、入出力バッファ7a2、およびセンスアンプなどの周辺回路を含んでいる。

[0130] 制御回路7b、CPU2から入力される制御用信号を一時的に格納し、動作ロジックの制御を行う。制御回路7bには、プロテクト処理制御部31が設けられている。

[0131] プロテクト処理制御部31は、フラッシュメモリ7におけるプロテクトエリアPAの領域を任意に変更する制御を行う。また、プロテクトエリアPAには、プロテクトエリアPAの先頭アドレスを格納する先頭アドレス格納エリアSDA、プロテクトエリアPAの末尾アドレスを格納する末尾アドレス格納エリアMDA、およびキーコードエリアを格納するキーコードエリアKAが設けられている。

[0132] プロテクト処理制御部31は、プロテクト処理制御回路32、アドレス生成回路33、リ

ード信号生成回路34、アドレス／キーコード格納レジスタ35、およびセクタ36、37から構成されている。

[0133] プロテクト処理制御回路32、アドレス生成回路33、リード信号生成回路34、およびアドレス／キーコード格納レジスタ35には、リセット信号を発生するリセット回路38から出力されたリセット信号が入力されるようにそれぞれ接続されている。

[0134] プロテクト処理制御回路32には、アドレス生成回路33、リード信号生成回路34、ならびにアドレス／キーコード格納レジスタ35がそれぞれ接続されており、該プロテクト処理制御回路32から出力された信号により、これらの回路が動作を開始する。

[0135] アドレス生成回路33は、フラッシュメモリ7のメモリマツ7aに格納されているキーコードの格納アドレスを生成する。リード信号生成回路34は、メモリマツ7aのリード信号を生成する。アドレス／キーコード格納レジスタ35は、メモリマツ7aから読み出したキーコード、およびプロテクトエリアPAの領域を示すアドレスをそれぞれ格納する。

[0136] またプロテクト処理制御回路32には、セクタ36、37を制御する制御信号が入力されるようにそれぞれ接続されている。セクタ36は、プロテクト処理制御回路32から出力される制御信号に基づいて、アドレス生成回路33が生成したアドレスと、バスステートコントローラ3から出力されるアドレスとを切り替えて出力する。

[0137] セクタ37は、プロテクト処理制御回路32から出力される制御信号に基づいて、リード信号生成回路34が生成したリード信号と、バスステートコントローラ3から出力されるリード信号とを切り替えて出力する。

[0138] 図14は、半導体集積回路装置1におけるリセットシーケンスを示した説明図であり、図15は、図14のリセットシーケンスにおけるプロテクト処理制御部31の設定処理を示すフローチャートである。

[0139] 図14においては、上方から下方にかけて、システムクロック、半導体集積回路装置1のリセット端子に入力されるリセット信号、プロテクト処理制御部31の動作状態、半導体集積回路装置1の内部路セット信号、およびCPU2(半導体集積回路装置1)の動作状態をそれぞれ示している。

[0140] まず、半導体集積回路装置の外部ポートの1つであるリセット端子からリセット信号が入力され、そのリセット信号が解除となると(ステップS501)、プロテクト処理制御回



路32が起動する(ステップS502)。

[0141] プロテクト処理制御回路32は、アドレス生成回路33、ならびにリード信号生成回路34に対して信号を出力し、これらアドレス生成回路33、およびリード信号生成回路34を動作させる(ステップS503)。

[0142] 続いて、プロテクト処理制御回路32は、メモリマップ7aのキーコードエリアKAに格納されているデータを読み出し(ステップS504)、そのデータをアドレス／キーコード格納レジスタ35に格納する(ステップS505)。

[0143] そして、プロテクト処理制御回路32は、アドレス／キーコード格納レジスタ35にキーコード(第1の設定値)が格納されているか否かを判断し(ステップS506)、キーコードが格納されている場合、プロテクト処理制御回路32は、メモリマップ7aからプロテクトエリアPAの先頭アドレスと末尾アドレスとを読み出して、アドレス／キーコード格納レジスタ35にそれぞれ格納する(ステップS507, S508)。

[0144] ステップS508の処理の終了後、またはステップS506の処理においてキーコードがない場合には、半導体集積回路装置の内部リセットを解除する解除信号をリセット回路38に出力した後(ステップS509)、プロテクト処理制御回路32が停止して(ステップS510)半導体集積回路装置1が動作を開始することになる。

[0145] キーコードの読み出しおよび制御回路7bに対するキーコードの設定、プロテクトエリアに対するプロテクトの有無の確認は、リセット解除後に上記フローに従って実行される。半導体集積回路装置1が通常の動作を開始した後は、図4に従ったメモリアクセスアドレスに基づいた制御を実行する。

[0146] また、プロテクトエリアPAおよびプロテクトエリアPA1がそれぞれ固定的な一つの領域とする場合はステップS507, S508は実行されない。

[0147] また、図16は、フラッシュメモリ7におけるプロテクトエリアPAの任意設定処理を示すフローチャートであり、図17は、図16におけるフラッシュメモリ7のメモリマップの補足説明図である。

[0148] まず、プログラムのデバッグを開始し(ステップS601)、プログラム書き込みと消去(ステップS602)をデバッグが完了するまで行う(ステップS603)。そして、デバッグが完了すると、メモリマップ7aに設けられた先頭アドレス格納エリアSDA、および末尾ア

ドレス格納エリアMDAにプロテクトエリアPAの任意の先頭アドレスと任意の末尾アドレスとをそれぞれ書き込み、プロテクトエリアPAの任意の領域を設定するとともに、キーコードエリアKAにキーコードを書き込む(ステップS604)。

[0149] この場合、先頭アドレス格納エリアSDA、末尾アドレス格納エリアMDAに、ならびにキーコードエリアKAがプロテクトエリアPAの領域内となるように、先頭アドレスと末尾アドレスとをそれぞれ設定することにより、第三者による該プロテクトエリアの領域変更読み出し、あるいはキーコードの読み出しや変更などを防止することができる。

[0150] それにより、本実施の形態2によれば、プロテクトエリアPAの領域を任意変更することができるので、読み出しや書き換えなどを禁止したいプログラムのデータ容量などに応じてフレキシブルに変更することが可能となるとともに、第三者によるプログラムの読み出しやコピー、あるいは変更などを防止することができる。

[0151] 以上、本発明者によってなされた発明を実施の形態に基づき具体的に説明したが、本発明は前記実施の形態に限定されるものではなく、その要旨を逸脱しない範囲で種々変更可能であることはいうまでもない。

#### 産業上の利用可能性

[0152] 本発明の半導体集積回路装置は、不揮発性半導体メモリにおける所定のブロックの読み出し、および書き換えを防止する技術に適している。

## 請求の範囲

- [1] 複数の不揮発性メモリセルを有するメモリアレイ部と、前記不揮発性メモリセルに情報を格納する書き込み動作、前記不揮発性メモリセルに格納した情報を読み出す読み出し動作、前記不揮発性メモリセルに格納した情報を消去する消去動作の各動作を制御する制御部とを備えた不揮発性記憶部と、前記不揮発性記憶部に格納されたプログラムのワークエリアとして用いられる揮発性記憶部と、所定の処理を実行し、前記不揮発性記憶部に動作指示を行うことが可能である中央処理装置と、前記不揮発性記憶部、および前記揮発性記憶部の読み出し動作を制御するプロテクト動作制御部とを有した半導体集積回路装置であって、

前記メモリアレイ部は、前記プロテクト動作制御部の制御により格納された情報の読み出し、および書き込みが禁止される第1のプロテクトメモリ領域を有し、

前記揮発性記憶部は、前記プロテクト動作制御部の制御により前記メモリアレイ部の第1のプロテクトメモリ領域以外からの読み出しが禁止される第2のプロテクトメモリ領域を有し、

前記不揮発性記憶部の第1のプロテクトメモリ領域に格納されたプログラムのワークエリアとして揮発性記憶部の第2のプロテクトメモリ領域を用いることを特徴とする半導体集積回路装置。

- [2] 複数の不揮発性メモリセルを有するメモリアレイ部と、前記不揮発性メモリセルに情報を格納する書き込み動作、前記不揮発性メモリセルに格納した情報を読み出す読み出し動作、前記不揮発性メモリセルに格納した情報を消去する消去動作の各動作を制御する制御部とを備えた不揮発性記憶部と、揮発性記憶部と、所定の処理を実行し、前記不揮発性記憶部に動作指示を行うことが可能である中央処理装置と、前記不揮発性記憶部、および前記揮発性記憶部の読み出し動作を制御するプロテクト動作制御部とを有した半導体集積回路装置であって、

前記メモリアレイ部は、前記プロテクト動作制御部の制御により格納された情報の読み出し、および書き込みが禁止される第1のプロテクトメモリ領域を有し、

前記揮発性記憶部は、前記プロテクト動作制御部の制御により前記メモリアレイ部の第1のプロテクトメモリ領域以外からの読み出し、および書き込みが禁止される第2

のプロテクトメモリ領域を有したことを特徴とする半導体集積回路装置。

- [3] 請求項1または2記載の半導体集積回路装置において、  
前記プロテクト動作制御部は、  
前記中央処理装置から出力されるアドレス信号とプログラムカウンタとの値を比較して前記第1のプロテクトメモリ領域であるか否かを判別することを特徴とする半導体集積回路装置。
- [4] 請求項3記載の半導体集積回路装置において、  
前記プロテクト動作制御部は、  
前記中央処理装置から出力されるアドレス信号とプログラムカウンタとの値を比較し、それらアドレス信号、およびプログラムカウンタの値がいずれも前記第1のプロテクトメモリ領域内のアドレス値である場合のみ、前記第1のプロテクトメモリ領域の読み出しを許可することを特徴とする半導体集積回路装置。
- [5] 請求項1〜4のいずれか1項に記載の半導体集積回路装置において、  
前記プロテクト動作制御部は、  
前記中央処理装置から出力されるアドレス信号とプログラムカウンタとの値を比較して前記第2のプロテクトメモリ領域であるか否かを判別することを特徴とする半導体集積回路装置。
- [6] 請求項5記載の半導体集積回路装置において、  
前記プロテクト動作制御部は、  
前記中央処理装置から出力されるアドレス信号とプログラムカウンタとの値を比較し、プログラムカウンタの値が前記第1のプロテクトメモリ領域内にあり、かつアドレス信号が前記第2のプロテクトメモリ領域内のアドレス値である場合のみ、前記第2のプロテクトメモリ領域の読み出しを許可することを特徴とする半導体集積回路装置。
- [7] 請求項1〜6のいずれか1項に記載の半導体集積回路装置において、  
前記第1のプロテクトメモリ領域における消去を禁止する消去禁止制御部を備えたことを特徴とする半導体集積回路装置。
- [8] 請求項7記載の半導体集積回路装置において、  
前記消去禁止制御部は、

- 予め設定されたキーコード信号を出力するキーコード発生回路と、  
前記メモリアレイ部の消去動作が発生した際に、前記キーコード発生回路が生成したキーコード信号と、前記第1のプロテクトメモリ領域に格納されたキーコードとを比較し、それらキーコードが一致した際に前記第1のプロテクトメモリ領域における消去を禁止する消去制御回路とを備えたことを特徴とする半導体集積回路装置。
- [9] 請求項1〜8のいずれか1項に記載の半導体集積回路装置において、  
前記第1のプロテクトメモリ領域における書き換えを禁止する書き換え禁止制御部を備えたことを特徴とする半導体集積回路装置。
- [10] 請求項9記載の半導体集積回路装置において、  
前記書き換え禁止制御部は、  
予め設定されたキーコード信号を出力するキーコード発生回路と、  
書き換え先アドレス信号が前記第1のプロテクトメモリ領域内か否かを判定するアドレス判定部と、  
前記キーコード発生回路が生成したキーコード信号と前記第1のプロテクトメモリ領域に格納されたキーコードとを比較し、それらキーコードが一致した際に一致信号を出力するキーコード判定部と、  
前記メモリアレイ部の書き換え動作が発生した際に、書き換え先アドレス信号が前記第1のプロテクトメモリ領域内であり、かつキーコードが一致した場合に前記第1のプロテクトメモリ領域の書き換えを禁止する書き換え禁止信号を出力する書き換え制御回路とを備えたことを特徴とする半導体集積回路装置。
- [11] 複数の不揮発性メモリセルを有するメモリアレイ部と、前記不揮発性メモリセルに情報を格納する書き込み動作、前記不揮発性メモリセルに格納した情報を読み出す読み出し動作、前記不揮発性メモリセルに格納した情報を消去する消去動作の各動作を制御する制御部とを備えた不揮発性半導体記憶装置と、  
前記不揮発性半導体記憶装置に格納されたプログラムのワークエリアとして用いられる揮発性半導体記憶装置と、  
所定の処理を実行し、前記不揮発性半導体記憶装置に動作指示を行うことが可能である中央処理装置と前記不揮発性半導体記憶装置、および前記揮発性半導体記

憶装置の読み出し動作を制御するプロテクト動作制御部とを備えた半導体集積回路装置とを有した電子システムであって、

前記メモリアレイ部は、前記プロテクト動作制御部の制御により格納された情報の読み出しが禁止される第1のプロテクトメモリ領域を有し、

前記揮発性半導体記憶装置は、前記プロテクト動作制御部の制御により前記メモリアレイ部の第1のプロテクトメモリ領域以外からの読み出しが禁止される第2のプロテクトメモリ領域を有し、

前記不揮発性半導体記憶装置に格納されたプログラムのワークエリアとして前記第2のプロテクトメモリ領域を用いることを特徴とする電子システム。

[12] 請求項11記載の電子システムにおいて、

前記プロテクト動作制御部は、

前記中央処理装置から出力されるアドレス信号とプログラムカウンタとの値を比較して前記第1、および第2のプロテクトメモリ領域であるか否かを判別することを特徴とする電子システム。

[13] 請求項12記載の電子システムにおいて、

前記プロテクト動作制御部は、

前記中央処理装置から出力されるアドレス信号とプログラムカウンタとの値を比較し、それらアドレス信号、およびプログラムカウンタの値がいずれも前記第1のプロテクトメモリ領域内のアドレス値である場合に前記第1のプロテクトメモリ領域の読み出しを許可し、プログラムカウンタの値が前記第1のプロテクトメモリ領域内にあり、かつアドレス信号が前記第2のプロテクトメモリ領域内のアドレス値である場合に前記第2のプロテクトメモリ領域の読み出しを許可することを特徴とする電子システム。

[14] 請求項10～13のいずれか1項に記載の電子システムにおいて、

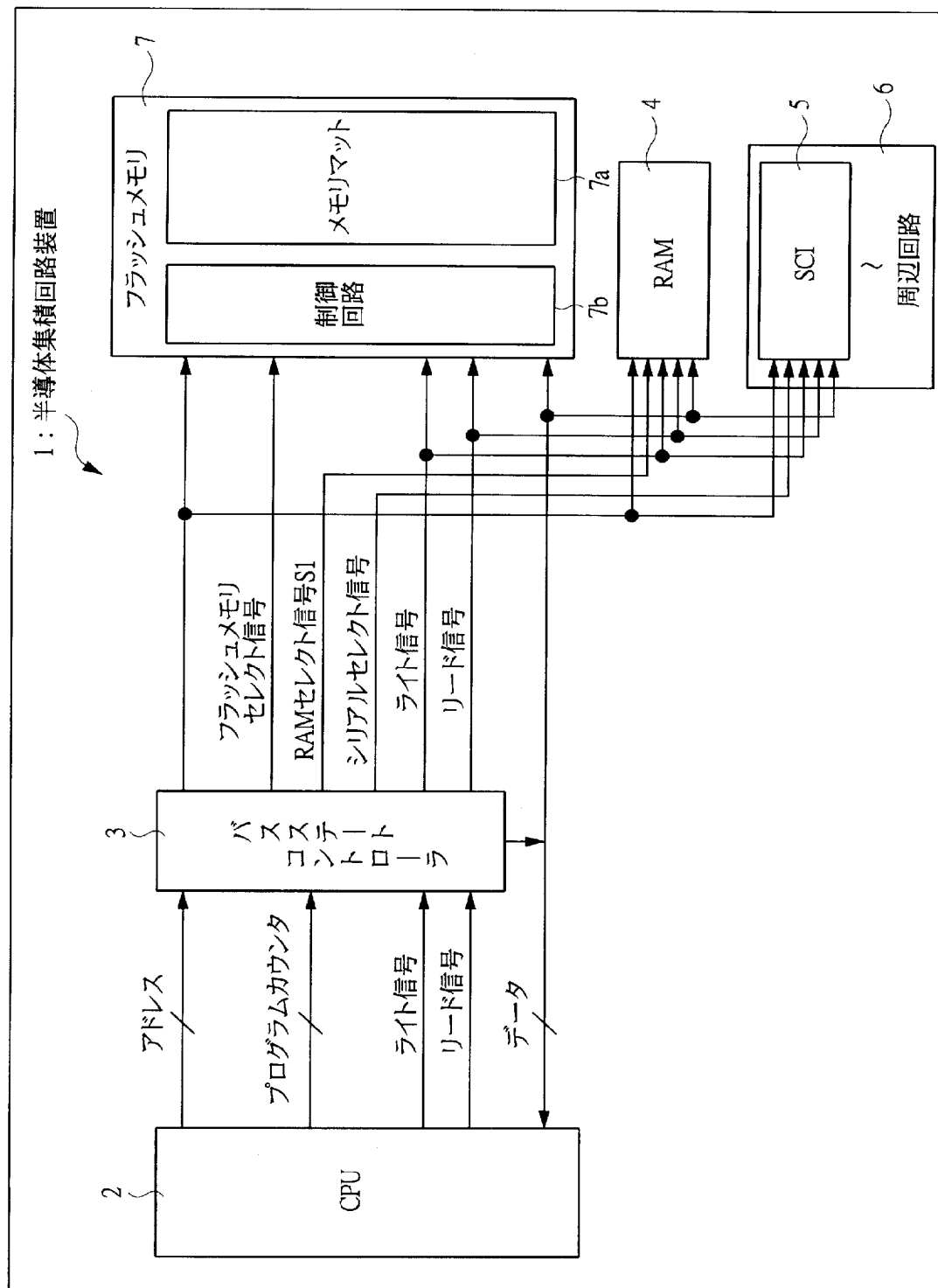
前記第1のプロテクトメモリ領域における消去を禁止する消去禁止制御部を備えたことを特徴とする電子システム。

[15] 請求項10～14のいずれか1項に記載の電子システムにおいて、

前記第1のプロテクトメモリ領域における書き換えを禁止する書き換え禁止制御部を備えたことを特徴とする電子システム。

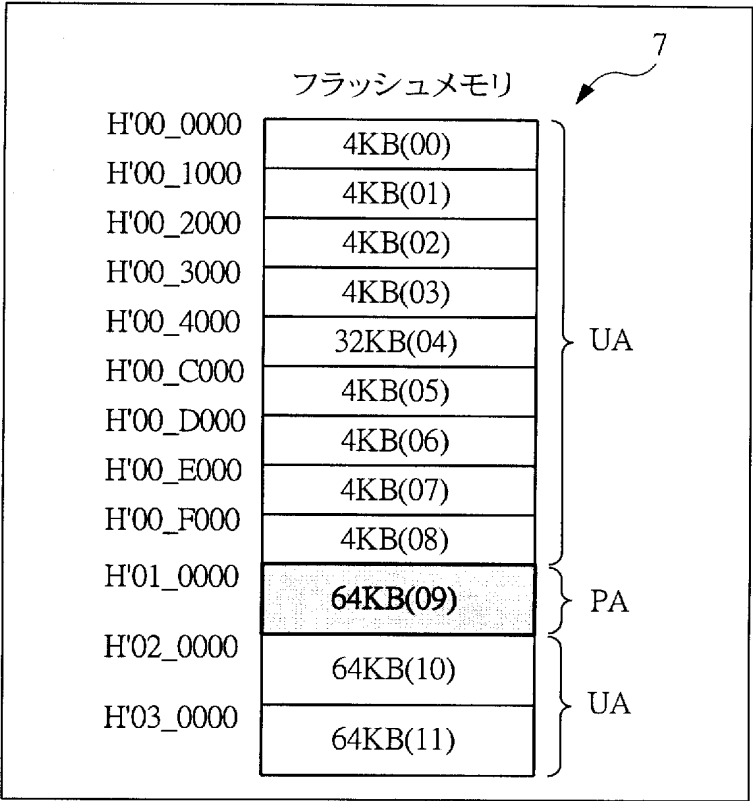
[図1]

図 1



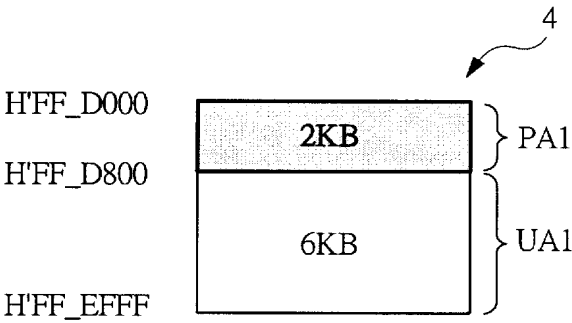
[[図2]

図 2



[[図3]

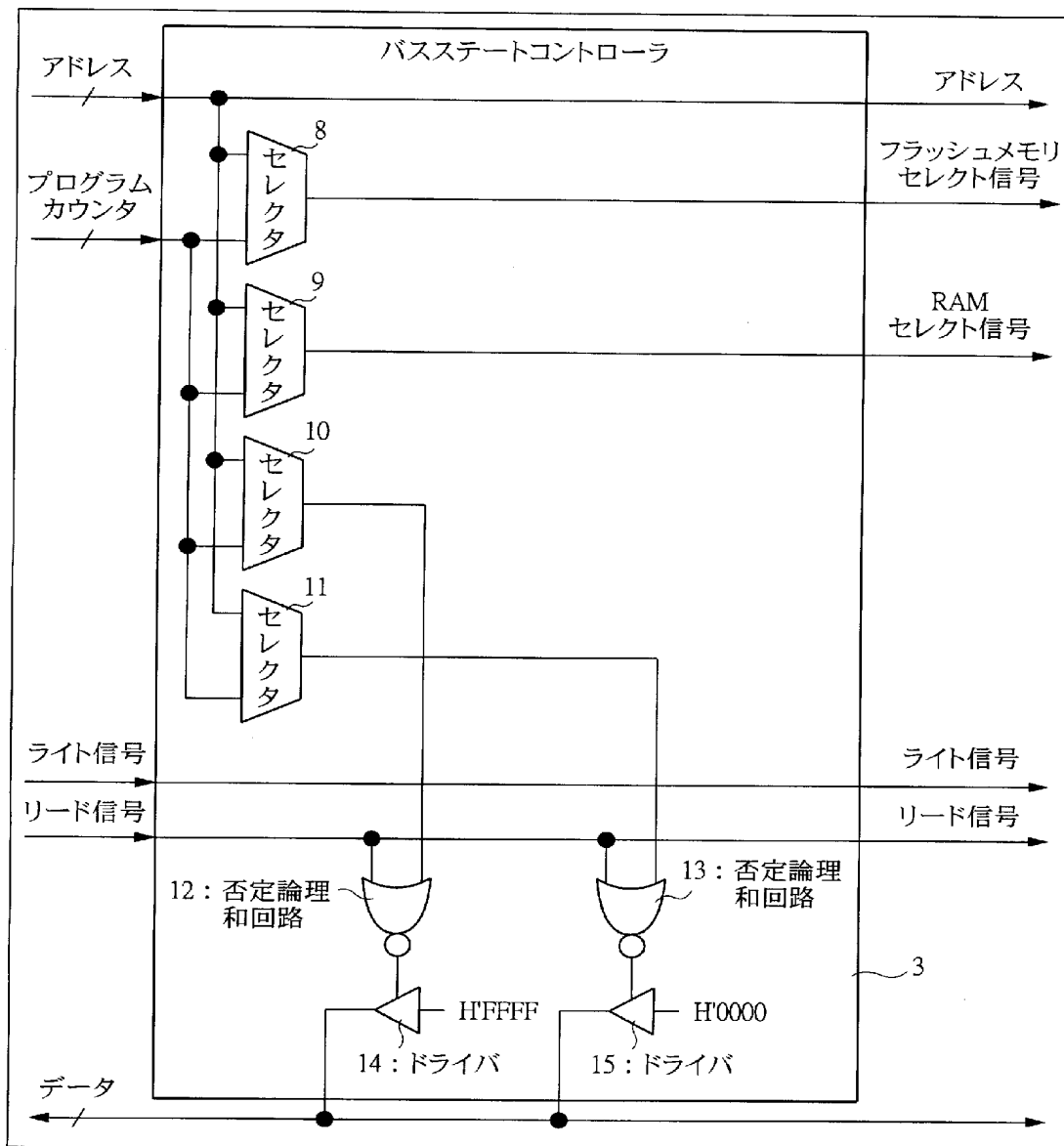
図 3





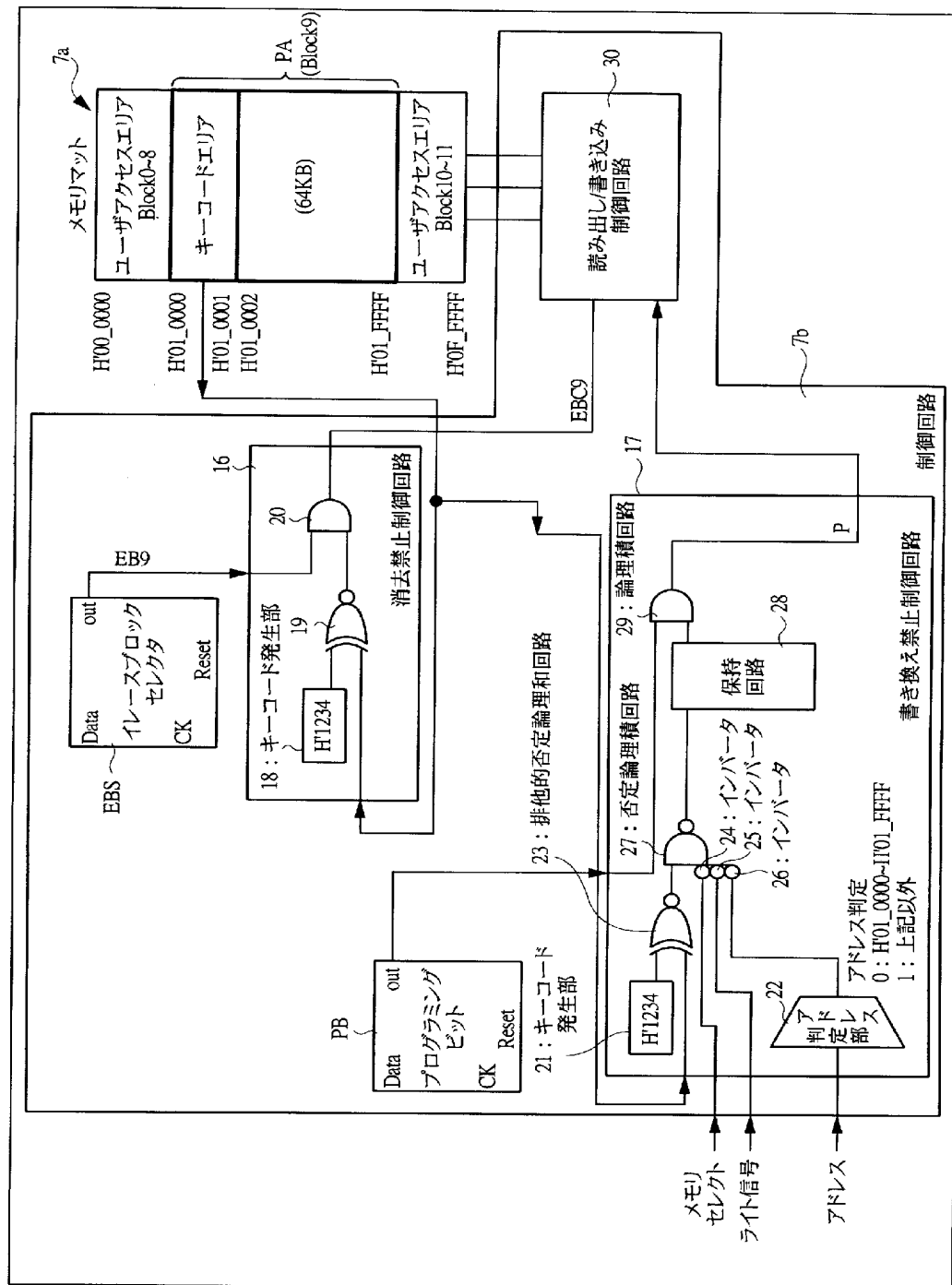
[図4]

図 4

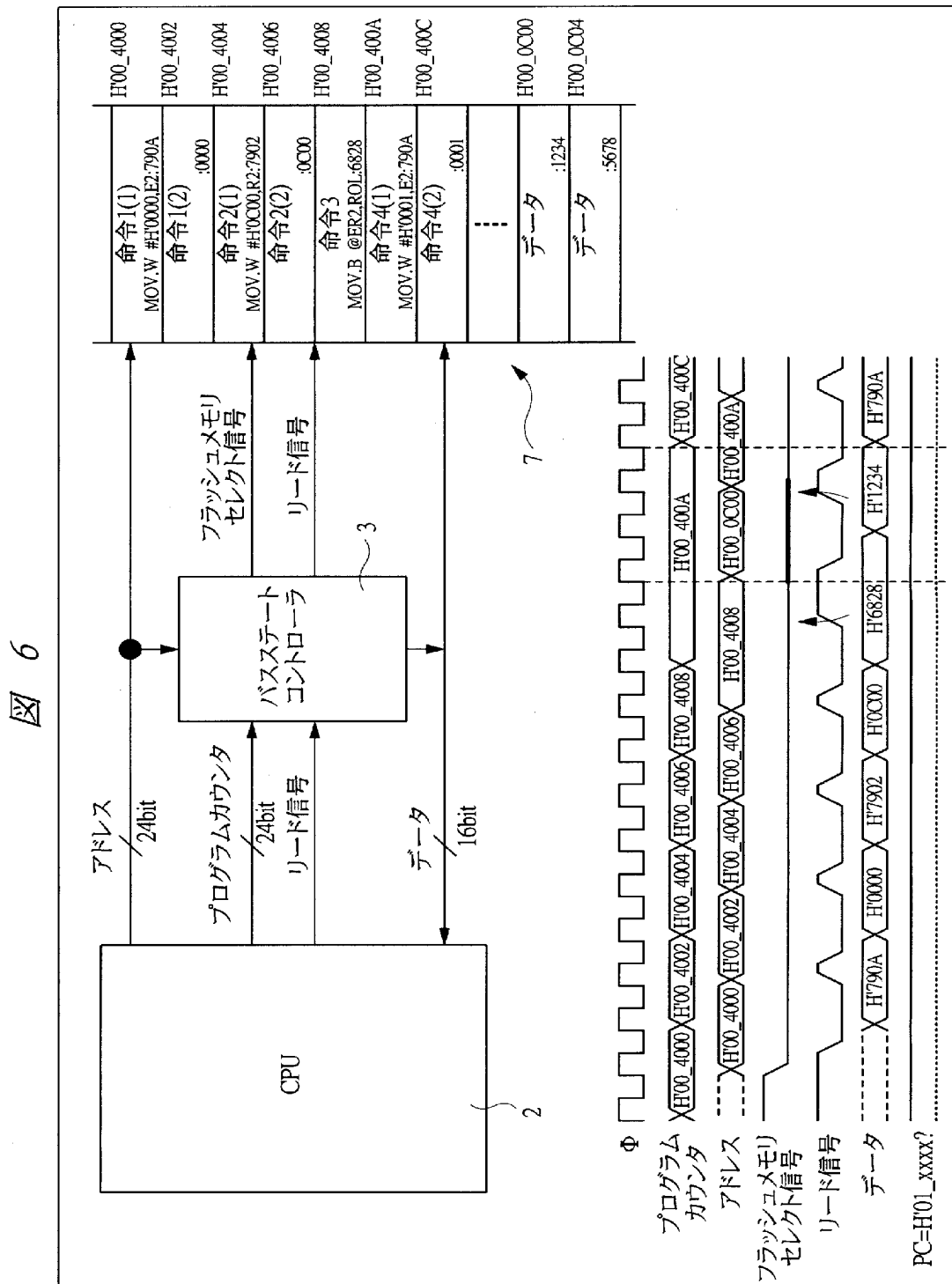


[図5]

図 5

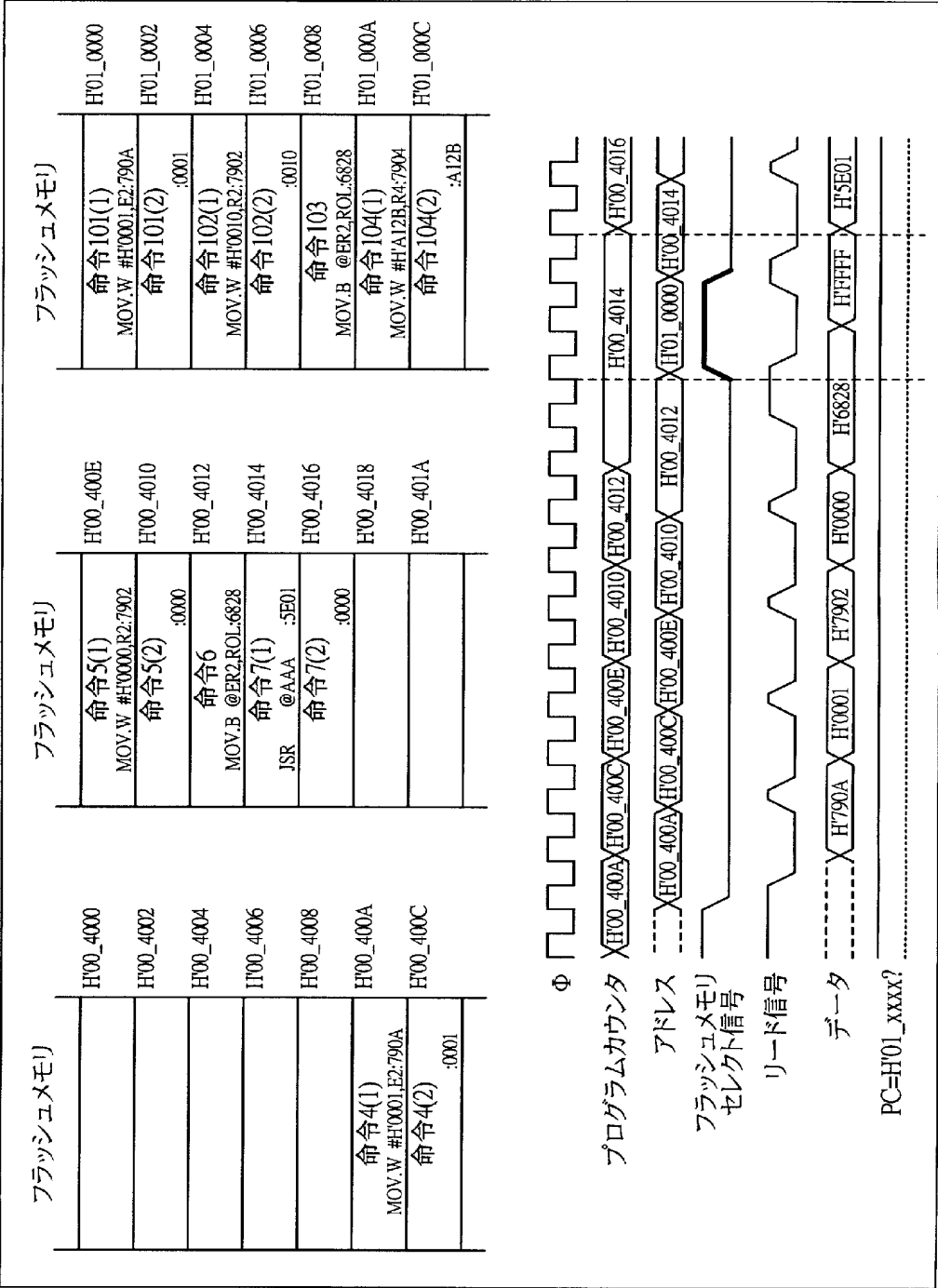


[図6]



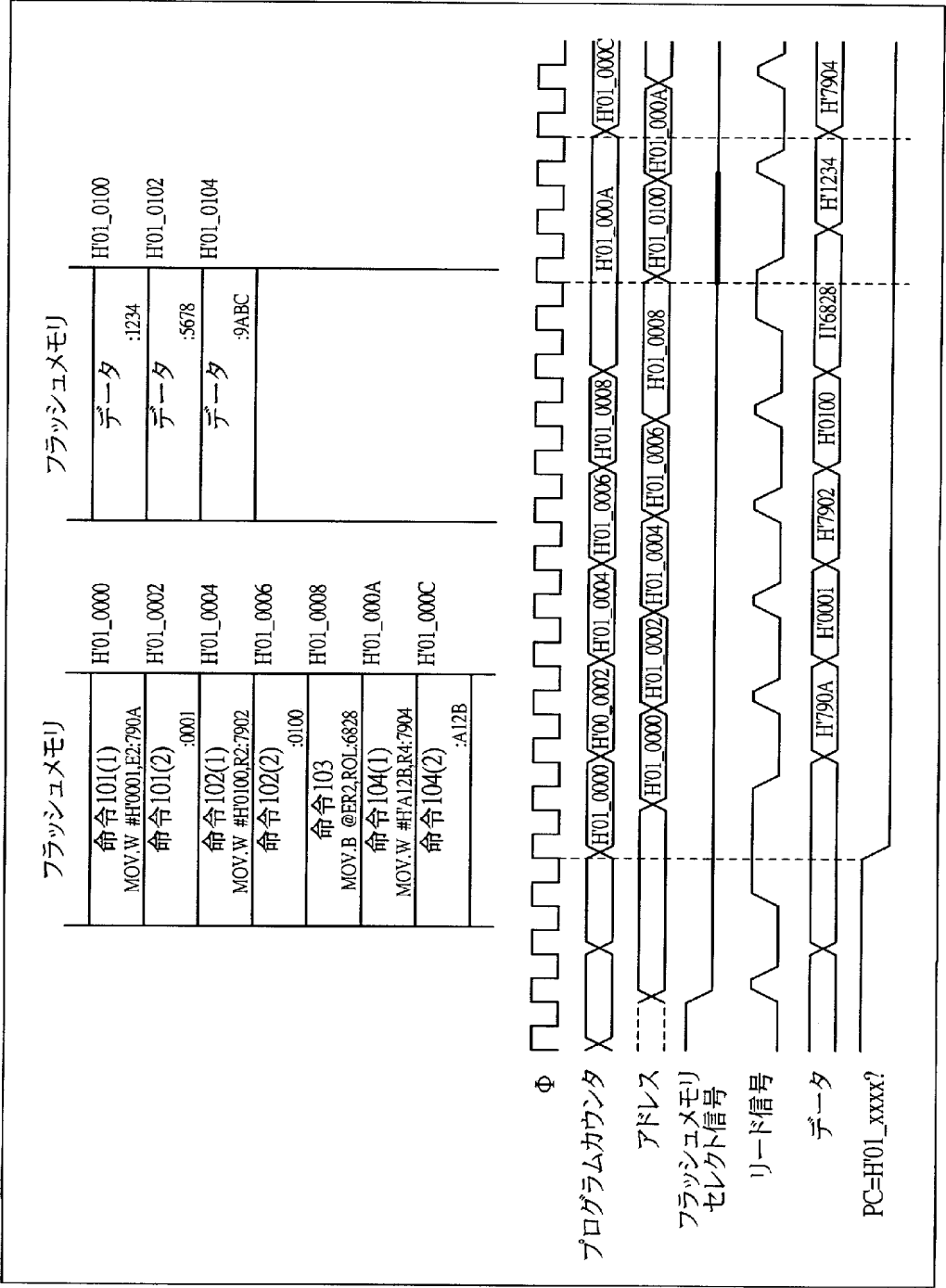
[図7]

図 7



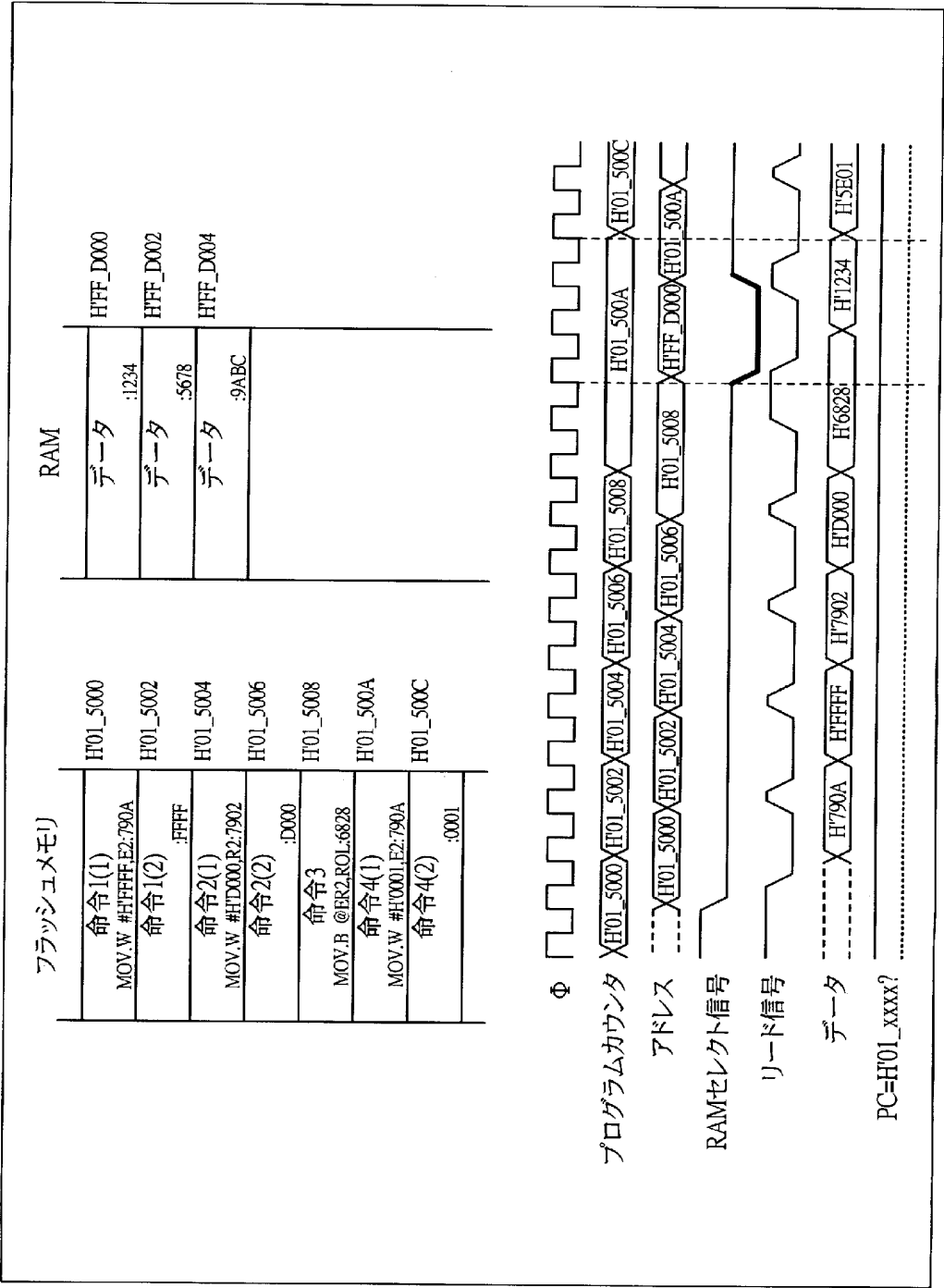
[図8]

図 8



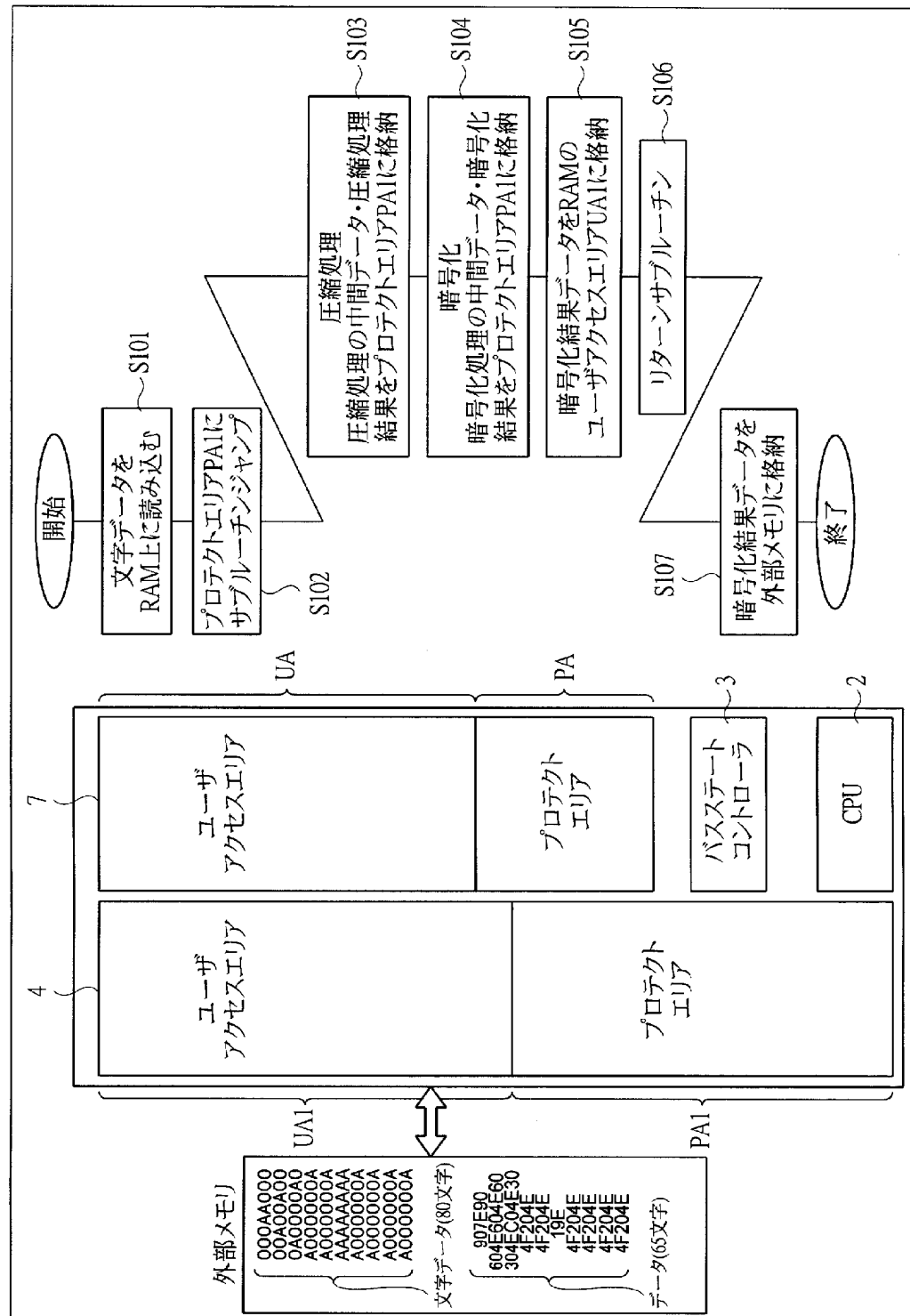
[図9]

図 9



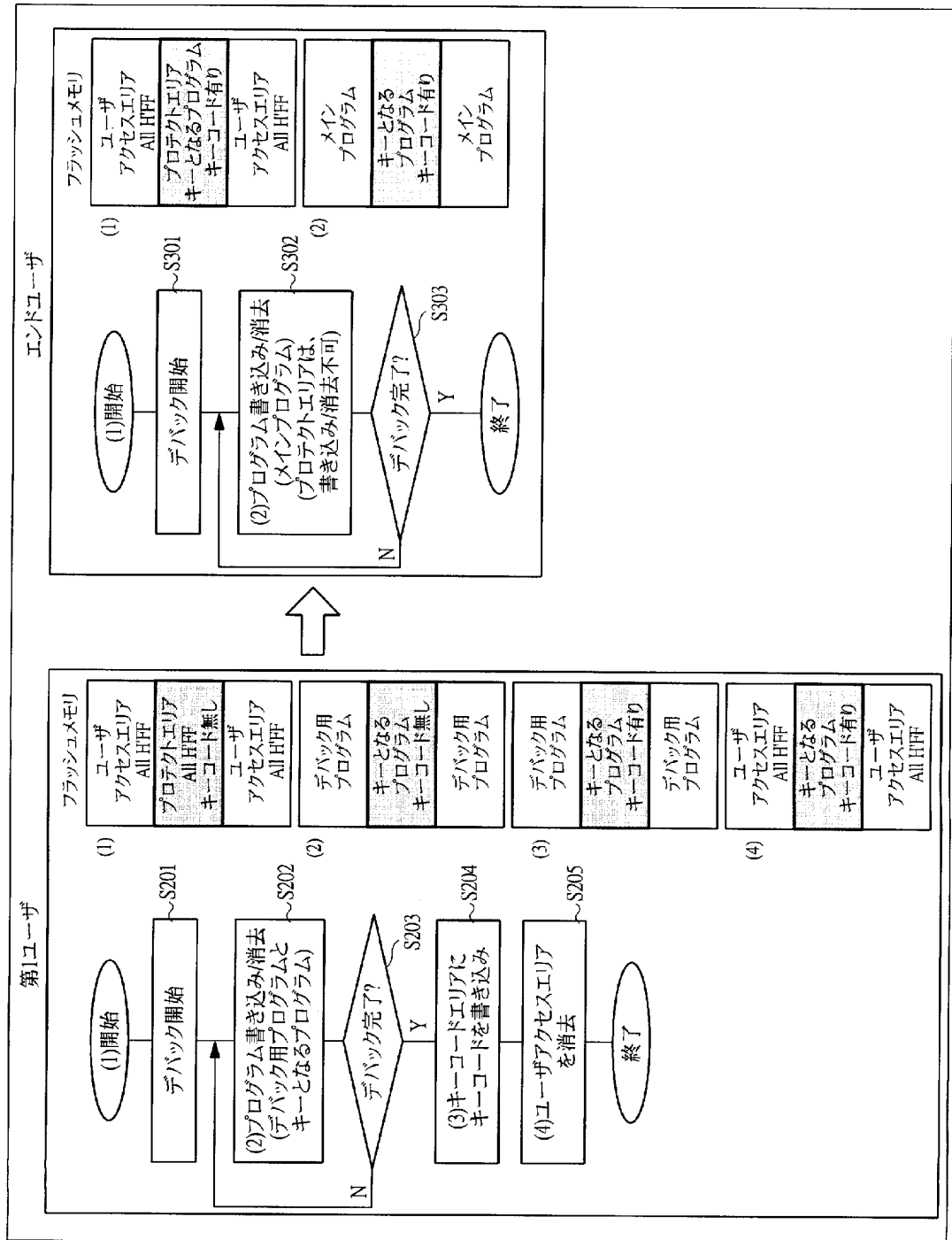
[図10]

図 10



[図11]

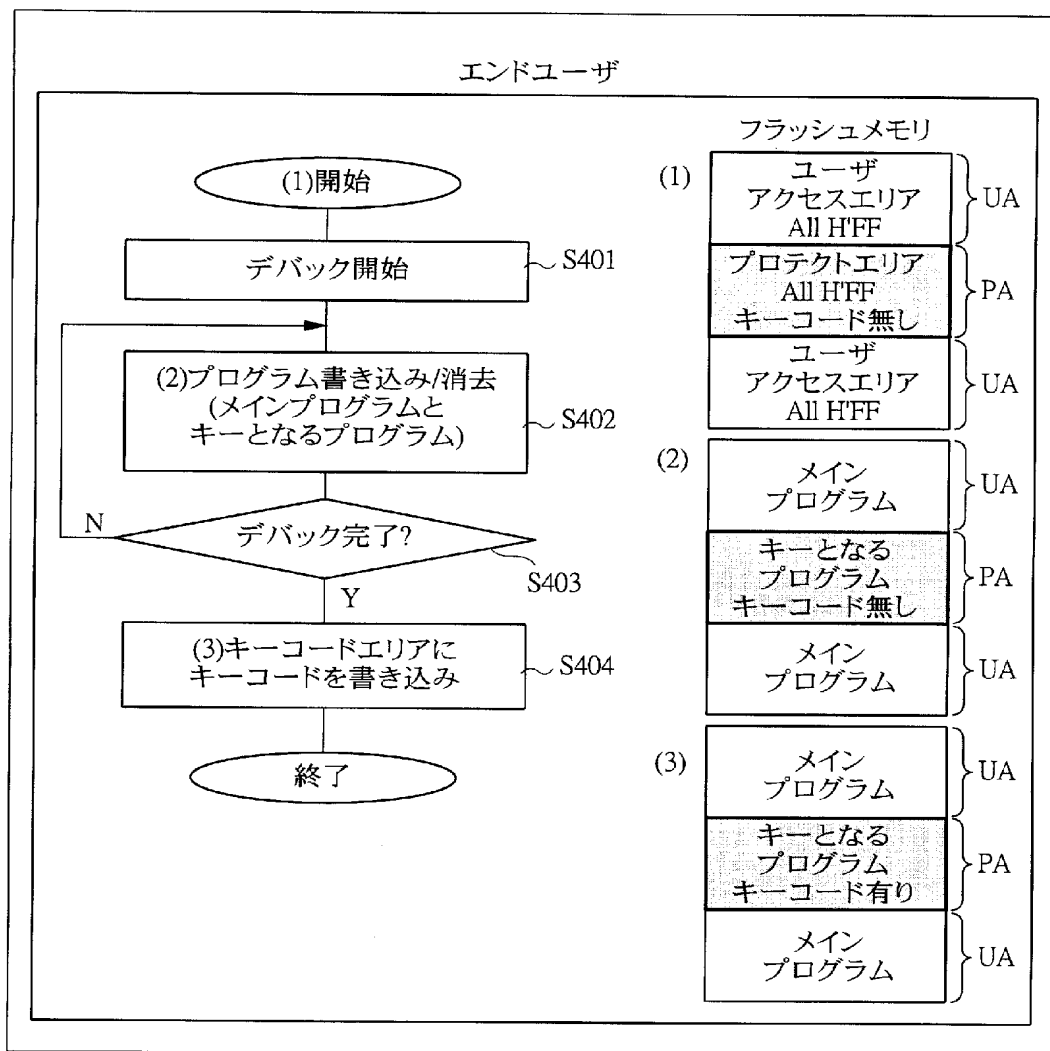
図 11





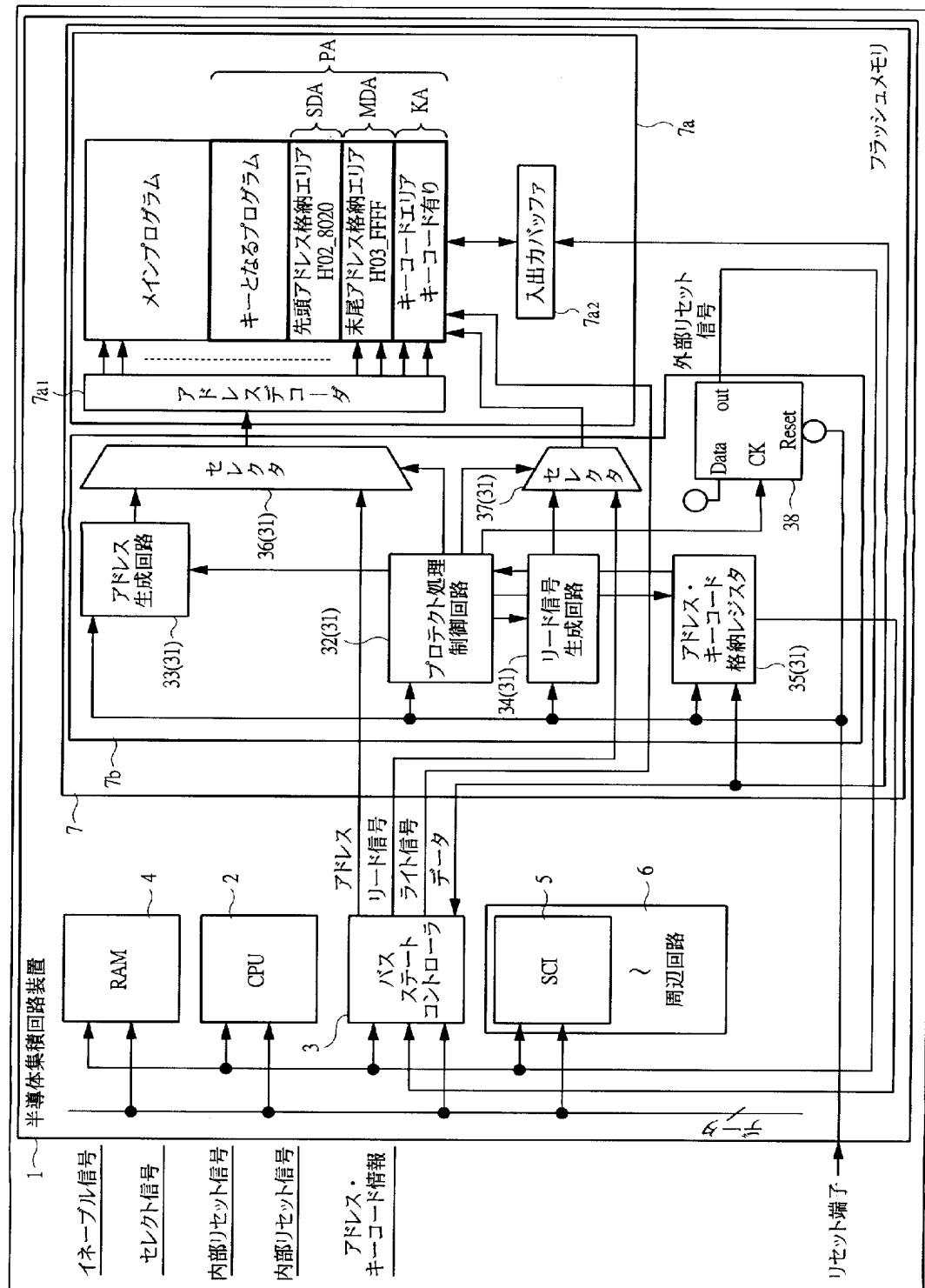
[図12]

図 12



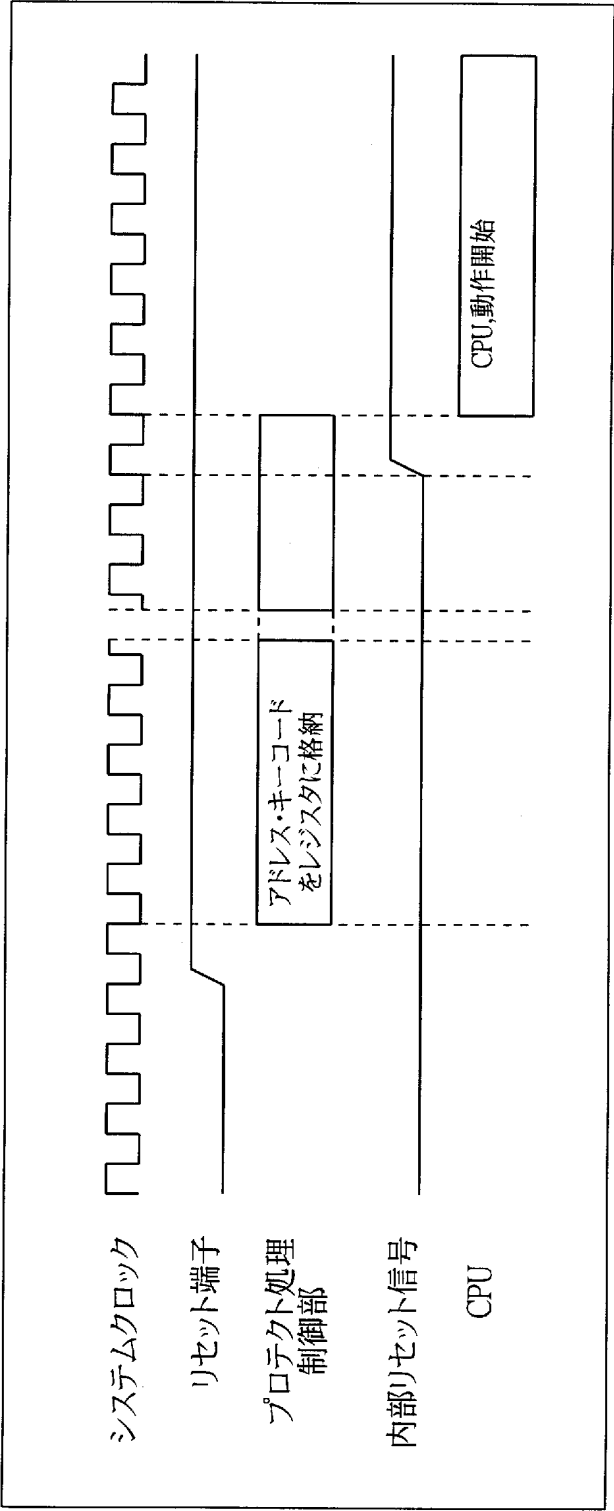
[図13]

図 13



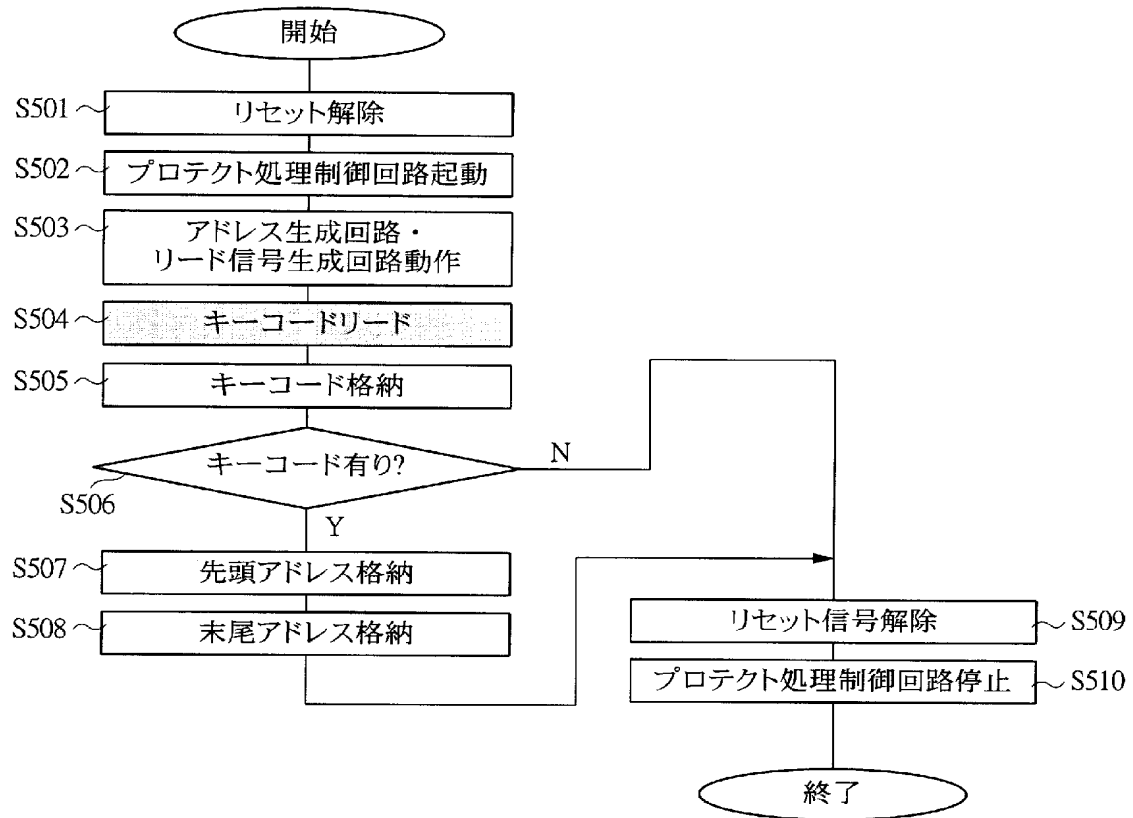
[図14]

図 14



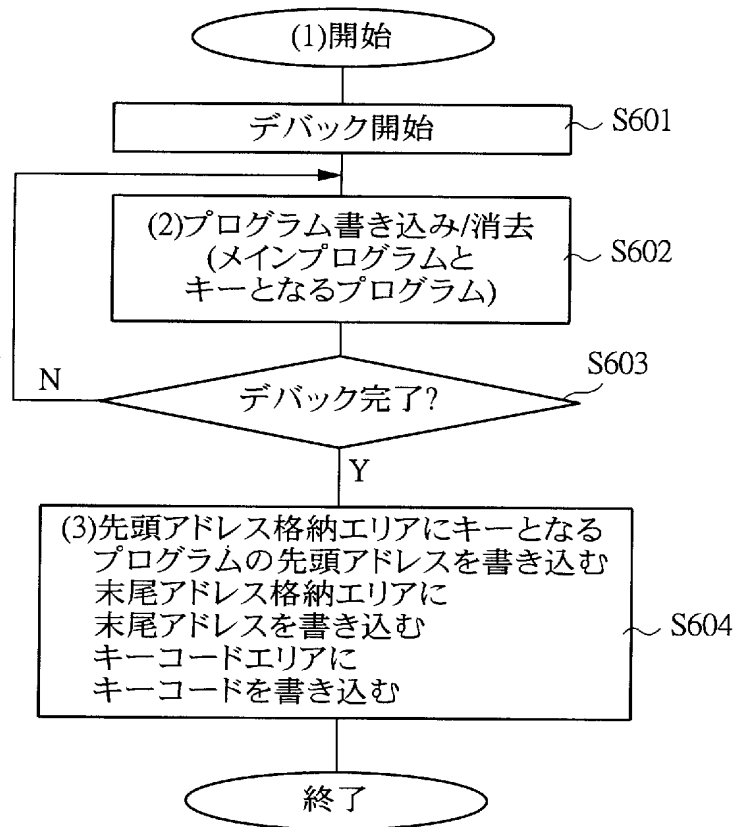
[図15]

図 15



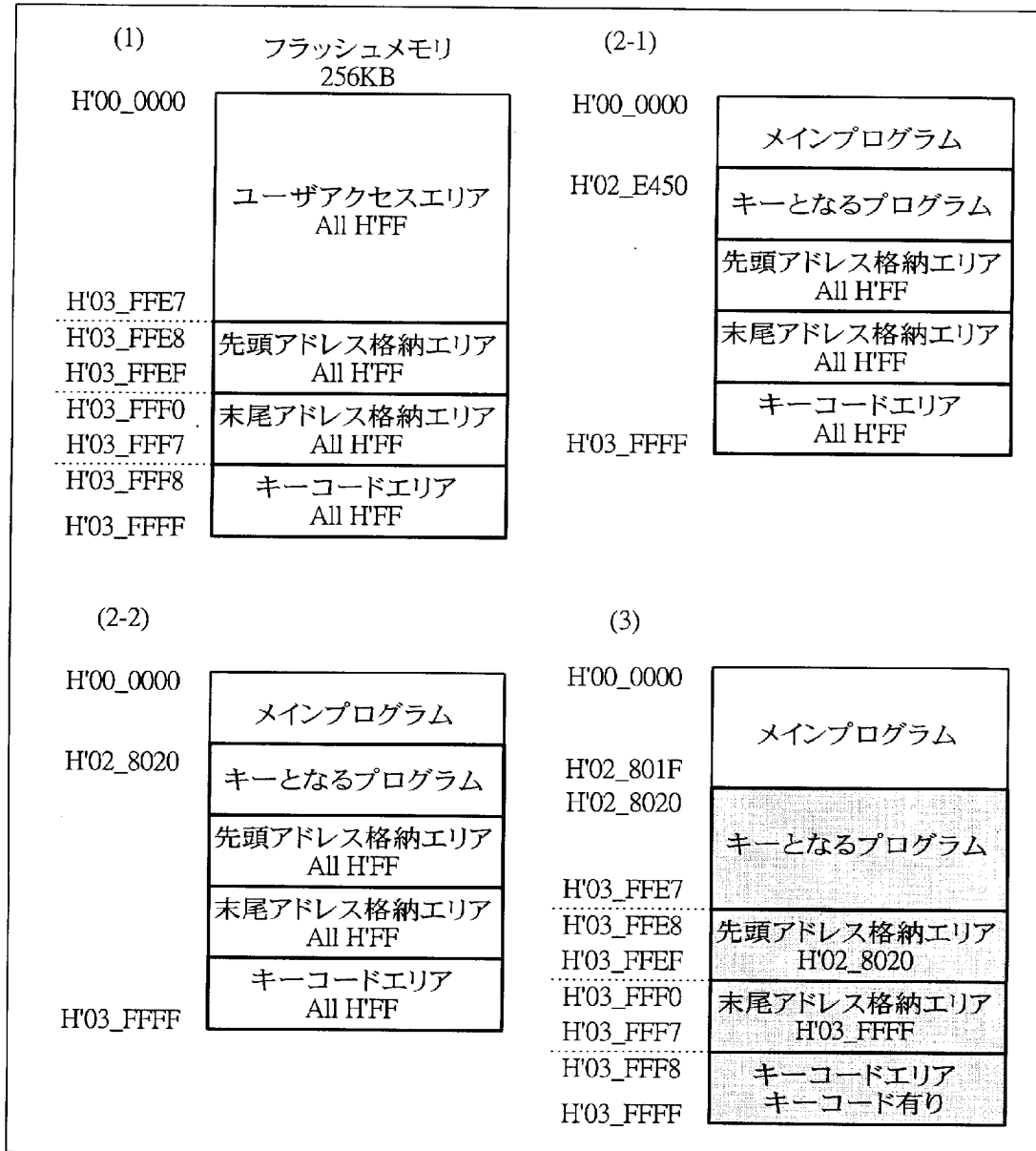
[図16]

図 16



[図17]

図 17



# INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2004/014939

## A. CLASSIFICATION OF SUBJECT MATTER

Int.Cl<sup>7</sup> G06F12/14

According to International Patent Classification (IPC) or to both national classification and IPC

## B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

Int.Cl<sup>7</sup> G06F12/14

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1922-1996	Jitsuyo Shinan Toroku Koho	1996-2004
Kokai Jitsuyo Shinan Koho	1971-2004	Toroku Jitsuyo Shinan Koho	1994-2004

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

## C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	JP 2004-145605 A (Matsushita Electric Industrial Co., Ltd.), 20 May, 2004 (20.05.04), Par. Nos. [0008] to [0028]; Figs. 1, 2, 4 (Family: none)	1-15
A	JP 10-228421 A (NEC IC Miconsystem Kabushiki Kaisha), 25 August, 1998 (25.08.98), Full text & EP 0859319 A1 & US 6101586 A	1-15

☐ Further documents are listed in the continuation of Box C.

☐ See patent family annex.

\* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance  
 "E" earlier application or patent but published on or after the international filing date  
 "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)  
 "O" document referring to an oral disclosure, use, exhibition or other means  
 "P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention  
 "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone  
 "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art  
 "&" document member of the same patent family

Date of the actual completion of the international search  
27 October, 2004 (27.10.04)

Date of mailing of the international search report  
16 November, 2004 (16.11.04)

Name and mailing address of the ISA/  
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

## A. 発明の属する分野の分類 (国際特許分類 (IPC))

Int. Cl.<sup>7</sup> G06F 12/14

## B. 調査を行った分野

調査を行った最小限資料 (国際特許分類 (IPC))

Int. Cl.<sup>7</sup> G06F 12/14

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報 1922-1996年

日本国公開実用新案公報 1971-2004年

日本国実用新案登録公報 1996-2004年

日本国登録実用新案公報 1994-2004年

国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)

## C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
X	JP 2004-145605 A (松下電器産業株式会社) 2004. 05. 20, 段落【0008】-【0028】, 第1 図, 第2図, 第4図 (ファミリーなし)	1-15
A	JP 10-228421 A (日本電気アイシーマイコンシステム 株式会社) 1998. 08. 25, 全文 & EP 0859319 A1 & US 6101586 A	1-15

☐ C欄の続きにも文献が列挙されている。☐ パテントファミリーに関する別紙を参照。

## \* 引用文献のカテゴリー

「A」 特に関連のある文献ではなく、一般的技術水準を示すもの

「E」 国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの

「L」 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す)

「O」 口頭による開示、使用、展示等に言及する文献

「P」 国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献

「T」 国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの

「X」 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの

「Y」 特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの

「&amp;」 同一パテントファミリー文献

国際調査を完了した日

27. 10. 2004

国際調査報告の発送日

16.11.2004

国際調査機関の名称及びあて先

日本国特許庁 (ISA/JP)

郵便番号100-8915

東京都千代田区霞が関三丁目4番3号

特許庁審査官 (権限のある職員)

平井 誠

5N

9071

電話番号 03-3581-1101 内線 3545